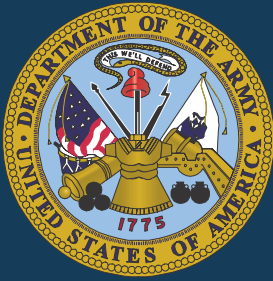


Joint Publication 3-04



Information in Joint Operations



14 September 2022



PREFACE

1. Scope

This publication provides fundamental principles and guidance to plan, coordinate, execute, and assess the use of information during joint operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS). It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and it provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations and training. It provides military guidance for use by the Armed Forces of the United States in preparing and executing their plans and orders. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of objectives.

3. Application

a. Joint doctrine established in this publication applies to the Joint Staff, commanders of combatant commands, subordinate unified commands, joint task forces, subordinate components of these commands, the Services, the National Guard Bureau, and combat support agencies.

b. This doctrine constitutes official advice concerning the enclosed subject matter; however, the judgment of the commander is paramount in all situations.

c. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the CJCS, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance

or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with United States law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

A handwritten signature in blue ink, reading "Dagvin R. M. Anderson". The signature is fluid and cursive, with the first name "Dagvin" being the most prominent.

DAGVIN R. M. ANDERSON
Lieutenant General, U.S. Air Force
Director for Joint Force Development

TABLE OF CONTENTS

EXECUTIVE SUMMARY	vii
-------------------------	-----

CHAPTER I FUNDAMENTALS OF INFORMATION

• Overview	I-1
• The Security Environment	I-2
• Information	I-5

CHAPTER II JOINT FORCE USES OF INFORMATION

• Military Operations and Information	II-1
• The Operational Environment and the Information Environment	II-1
• Information Advantage	II-2
• Informational Power	II-2
• Relevant Actors	II-5
• Joint Force Use of Narrative	II-5
• The Information Joint Function	II-6
• The Information Joint Function and Joint Operations	II-15

CHAPTER III UNITY OF EFFORT

• Introduction	III-1
• Authorities	III-2
• Responsibilities	III-3
• Service Organizations	III-23
• Information Forces	III-27
• Interorganizational Collaboration	III-29
• Multinational Partner Considerations	III-31
• Legal Considerations	III-33

CHAPTER IV OPERATIONAL DESIGN AND PLANNING

• Introduction	IV-1
• Information Planners and Operational Design and Planning	IV-1
• Operational Design	IV-2
• Joint Planning Process	IV-14

CHAPTER V
EXECUTION

- Introduction..... V-1
- Execution in Context V-1
- Essential Elements for Incorporating Information into Execution..... V-1

CHAPTER VI
ASSESSMENT

- Introduction..... VI-1
- Requirement for Assessment VI-1
- Challenges Assessing Information in Joint Operations VI-2
- Organizing for Assessment VI-3
- Assessment Process VI-4
- Recommendations for Assessing Inform and Influence Activities VI-12

CHAPTER VII
OPERATIONS IN THE INFORMATION ENVIRONMENT

- Overview..... VII-1
- Operations in the Information Environment..... VII-1
- Organizing for Operations in the Information Environment VII-7
- Operations in the Information Environment Planning, Coordination,
Execution, and Assessment..... VII-11

APPENDIX

- A Narrative Development..... A-1
- B Information Staff Estimate Format..... B-1
- C Guide for the Integration of Information in Joint Operations..... C-1
- D References..... D-1
- E Administrative Instructions..... E-1
- F Classified Appendix (published separately) F-1

GLOSSARY

- Part I Shortened Word Forms (Abbreviations, Acronyms, and Initialisms).....GL-1
- Part II Terms and DefinitionsGL-5

FIGURE

- I-1 Examples of Inherent Informational Aspects..... I-6
- I-2 Examples of Drivers of Human Behavior..... I-7
- II-1 Tasks and Outcomes of the Information Joint Function..... II-7
- IV-1 Joint Planning Overview.....IV-3

IV-2	Narrative Hierarchy	IV-4
IV-3	Planning Functions, Process, and Operational Design Methodology	IV-15
IV-4	Questions for Narrative Analysis	IV-18
VI-1	Operation Assessment Process.....	VI-5
VI-2	Assessment Plan Development Process.....	VI-6
A-1	Potential Testing Pool.....	A-7
C-1	Guide for the Integration of Information in Joint Operations.....	C-2

Intentionally Blank

EXECUTIVE SUMMARY COMMANDER'S OVERVIEW

- Introduces the fundamentals of information in the context of the security environment
- Describes the joint forces use and leveraging of information through the information joint function during all joint operations
- Discusses the Department of Defense's role in maintaining unity of effort in and through the information environment
- Outlines information planners' contributions to operational design and planning
- Presents essential elements for incorporating information into execution
- Describes the requirement to, and challenges of, assessing the joint force's use and leveraging of information in joint operations, organizing for assessment, the assessment process, and recommendations for assessing inform and influence activities
- Discusses the planning, coordination, execution, and assessment of operations in the information environment and the forces that conduct those operations

Fundamentals of Information

Introduction

The Department of Defense (DOD), in coordination with the other United States Government departments and agencies, supports the informational instrument of national power by using information to impact the way in which humans and systems behave or function. The joint force leverages information across the competition continuum to assure, deter, compel, and force relevant actor behaviors that support United States (US) interests.

The information joint function organizes the tasks required for the management and application of information during all activities and operations. The three tasks of the information joint function stress the requirement to incorporate information as a foundational element during the planning and conduct of all operations. Those tasks are:

- Understand how information impacts the operational environment (OE).
- Support human and automated decision making.
- Leverage information.

The Security Environment

The security environment is the set of conditions, circumstances, and influences that affect the employment of the Armed Forces of the United States. It is impacted by advances in information technology that enable individuals and organizations to access, use, and share information across the globe; to interfere, alter, or disrupt the transmission of information; and to employ and deny information to affect individuals, groups, and automated systems worldwide.

Information

Information is data in context to which a receiver assigns meaning. Receivers include human and automated systems and each may acquire information in a variety of ways (e.g., through spoken or written words, observation, or some other sensing mechanism).

Humans use information to understand, make decisions, and communicate. Automated systems use information to support decision making, control their own functions, or control the behavior or functions of other systems. Humans and automated systems share information to establish a common understanding.

Information can affect behavior. Understanding the factors that drive behaviors is essential to the effective use of information. One can leverage information to affect drivers of behavior for automated systems by changing the algorithms, programs, and data that control the system's behavior (e.g., computer virus) or by sending information to the system's sensors to produce a predictable output (e.g., jamming a radar). Information can also affect human behavior. This is frequently more complicated because the drivers of behavior do not work in isolation—affecting any one driver can affect other drivers.

Joint Force Uses of Information

Military Operations and Information

The joint force uses information to improve understanding, decision making, and communication. Commanders use information to visualize and understand the OE and direct and coordinate actions.

The joint force leverages information to affect the perceptions, attitudes, decision making, and behavior of relevant actors.

The Operational Environment and the Information Environment (IE)

Within each commander's OE there exist factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information. We refer to the aggregate of these social, cultural, linguistic, psychological, technical, and physical factors as the information environment (IE). The IE is not distinct from any OE. It is an intellectual framework to help identify, understand, and describe how those often-intangible factors may affect the employment of forces and bear on the decisions of the commander.

Information Advantage

Information advantage is the operational advantage gained through the joint force's use of information for decision making and its ability to leverage information to create effects on the IE.

Informational Power

Informational power is the ability to use information to support achievement of objectives and gain an information advantage. The essence of informational power is the ability to exert one's will through the projection, exploitation, denial, and preservation of information in pursuit of objectives.

Relevant Actors

Relevant actors include individuals, groups, populations, or automated systems whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action.

Joint Force Use of Narrative

Narratives are an integral part of campaigns, operations, and missions. The joint force strives to provide a compelling narrative that is integrated into operation plans (OPLANs) and resonates with relevant actors by fitting their frame of reference. An effective and integrated narrative can mitigate, undermine, or otherwise render competing narratives ineffective if it is accompanied by complementary actions.

The Information Joint Function

The information joint function is the intellectual organization of the tasks required to use information during all operations—understand how information impacts the OE, support human and automated decision making, and leverage information. The information

joint function encompasses the management and application of information to change or maintain perceptions, attitudes, and other drivers of behavior and to support human and automated decision making.

The Information Joint Function and Joint Operations

The joint force commander (JFC) uses the abilities provided by the information joint function during all operations. The **understand task** provides the JFC with the ability to identify threats, vulnerabilities, and opportunities in the IE and provides a better understanding of which drivers of behavior to affect to achieve objectives. These activities facilitate the availability of timely, accurate, and relevant information necessary for joint force decision making. The **leverage task** provides the JFC with the ability to inform audiences; influence foreign relevant actors; and attack and exploit information, information networks, and information systems in support of the JFC's objectives and enduring outcomes. The joint force operationalizes the information joint function through operational design in planning of operations that use information and deliberately leverage the inherent informational aspects of its activities and by conducting operations in the information environment (OIE).

Operations in the Information Environment (OIE)

OIE are military actions involving the integrated employment of multiple information forces to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and protecting friendly information, information networks, and information systems.

Unity of Effort

Introduction

DOD's role in maintaining unity of effort in and through the IE is, for the most part, the same as it is for the physical domains. DOD establishes policies and sets the conditions for components and their staffs to identify adversarial and potential adversarial threats (including attempts to undermine US alliances and coalitions) and bring capabilities to bear in an effort to affect, undermine, and erode an adversary's or enemy's will.

Authorities

Military activities that leverage information frequently involve a unique set of complex issues. There are legal

and policy requirements, including DOD directives and instructions, national laws, international laws, and rules of engagement, all of which may affect these activities. Laws, policies, and guidelines become especially critical during peacetime operations and competition when international and domestic laws, treaty provisions, and agreements are more likely to affect planning and execution. Commanders should know who has the execution authority for the conduct of information activities since many capabilities require separate and distinct execution authorities.

Responsibilities

Information can have significant regional and global impacts that challenge the joint force with unanticipated threats, vulnerabilities, and opportunities. Effectively dealing with these challenges and communicating intended meanings to selected populations requires individuals and organizations across DOD and interagency partners to understand their own and others' responsibilities related to achieving and maintaining unity of effort in the application of informational power.

Service Organizations

The Services man, train, and equip organizations to provide the joint force with the ability to leverage information during joint operations and to conduct OIE. Those Service organizations provide distinct specialized capabilities to the joint force or provide information commands composed of multiple specialized capabilities that focus on leveraging information and enable the joint force to create effects in the IE. Those Service-provided organizations that are trained and equipped to conduct OIE are referred to as OIE units.

Information Forces

Information forces are those Active Component and Reserve Component forces of the Services specifically organized, trained, and equipped to create effects in the IE. These forces provide expertise and specialized capabilities that leverage information and can be aggregated as components of an OIE unit to conduct OIE. Information forces are available to the joint force through the request for forces process.

Interorganizational Collaboration

Interorganizational collaboration seeks to find common goals, objectives, and/or principles between diverse organizations to achieve unity of effort and, through planning and leveraging of cross-organizational capabilities, set the conditions to achieve unified action

during execution. The relationship that the joint force establishes with relevant organizations helps it develop a more comprehensive awareness of the OE and understanding of the impact of information on the OE.

Multinational Partner Considerations

There is no single doctrine for multinational action, and each alliance or coalition develops its own protocols and plans. With regard to information activities and the conduct of OIE, US planning for joint operations accommodates and complements the inherent complexity of multinational partner considerations.

Legal Considerations

US military information activities are subject to applicable international laws and treaties, US laws and policies, and DOD regulations and policies. Understanding how various policies and laws interact in practice with respect to the IE is a challenging task. To overcome these challenges, commanders and staff consult with legal advisors throughout the planning process. Planners should maintain awareness of relevant international agreements and consult with legal advisors to identify associated legal obligations/constraints that must be incorporated into plans.

Operational Design and Planning

Information Planners and Operational Design and Planning

Information planners assigned to the staff enhance the JFC staff's ability to carry out information joint function tasks. Those planners have subject matter expertise with specialized capabilities, experience working with and in OIE units, and an understanding of the inherent informational aspects of capabilities and activities of other units. Information planners collaborate with the rest of the staff to develop and plan activities in a manner that most effectively leverages the informational aspects of joint force operations, as well as planning OIE, to support achieving the JFC's objectives.

Operational Design

Operational design is the analytical framework that underpins planning. Operational design supports commanders and planners in understanding the JFC's OE as a complex interactive system. As commanders and staffs apply operational design methodology to develop the operational approach, they account for how information impacts the OE and the potential inherent informational aspects of their activities. In doing so, joint force planners gain an understanding of relevant

actors and consider how information is used by, and affects the behavior of, those actors.

Joint Planning Process

The joint planning process (JPP) is an orderly, analytical process that consists of a logical set of steps to analyze a mission, select the best course of action, and produce a campaign or joint OPLAN or order. Like operational design, it is a logical process to approach a problem and determine a solution.

Throughout the JPP steps, information planners assist other joint planners in incorporating their understanding of how information impacts the OE to identify how to best support human and automated system decision making and how to best leverage information to achieve the JFC's objectives during operations.

Execution

Execution in Context

Joint operations span the competition continuum from recurring cooperative activities to sustained combat operations in armed conflict. The information joint function enables the application of informational power by expanding commanders' range of options for action across the competition continuum. Employing the information joint function may be the primary option available to a JFC during long-duration cooperation and competition short of armed conflict, where the use of physical force is inappropriate or restricted.

Essential Elements for Incorporating Information into Execution

The JFC focuses on synchronizing, monitoring, and adjusting all joint force activities (i.e., not just information activities) so they have the desired effects in and through the IE and support achievement of joint and national objectives. The dynamic nature of the IE makes it vital that the JFC have the organizations, processes, and tools in place to rapidly recognize the informational aspects of activities and adapt joint force activities in response to failures or to exploit successes in and through the IE. The following are essential elements that facilitate that rapid adaptation:

- Organization.
- Monitoring and analyzing for effects in and through the IE.
- The synchronization matrix.
- The narrative.

- Information and knowledge management.
- The information staff estimate.

Assessment

Introduction

Assessing the joint force use and leveraging of information allows the JFC to appreciate whether those efforts are helping to achieve objectives. Assessment of joint force information activities is a continual and cyclical process.

Requirement for Assessment

Assessment of operations and activities is key to the commander's decision cycle, helping to determine the results of actions in the context of overall mission objectives and providing recommendations for refinement of future plans. Assessing the joint force's use and leveraging of information in joint operations provides data and analysis to inform the commander on how effectively the joint force is able to understand how information impacts the OE, support human and automated decision making, and leverage information to achieve objectives.

Challenges Assessing Information in Joint Operations

Distinguishing between correlation and causation makes information activity assessment difficult. Analysts should approach assessment with open minds and determine whether correlation, causality, or a combination of the two is the appropriate approach for specific measures of effectiveness. This approach provides insights to the likelihood of particular events and effects given certain criteria in terms of conditions and actors in the OE. When assessing information in joint operations, evidence has shown that correlation between indicators and events has proven more accurate than efforts to establish concrete cause and effects relationships. This is especially true when assessing public opinion or human behavior.

Organizing for Assessment

Three potential approaches for organizing for assessment are:

- **Special Staff Section.** In this approach, the assessment element reports directly to the commander, via the chief of staff or deputy commander.
- **Separate Staff Section.** In this approach, the assessment element is its own staff section, akin to

plans, operations, intelligence, logistics, and communications.

- **Integrated in Another Staff Section.** In this approach, the assessment element is typically integrated into the operations or plans sections and the assessment chief reports to the plans chief or the operations chief.

Assessment Process

Assessments of information in joint operations are conducted in accordance with the assessment process:

- **Step 1—Develop Assessment Approach**
- **Step 2—Develop Assessment Plan**
- **Step 3—Collect Information**
- **Step 4—Analyze Information and Produce Intelligence**
- **Step 5—Communicate Feedback and Recommendations**
- **Step 6—Adapt Plans for Operations, Campaigns, and Assessment**

Operations in the Information Environment

Introduction

OIE are military actions involving the integrated employment of multiple information forces to affect drivers of behavior. The forces that conduct OIE include OIE units (i.e., those formations that JFCs may choose to assemble to conduct OIE) and information forces, which are the building blocks of those OIE units.

Operations in the IE

OIE leverage information for the purpose of affecting the will, awareness, and understanding of adversaries and other relevant actors and denying them the ability to act in and through the IE to negatively affect the joint force, while protecting joint force will, awareness, understanding, and the ability to take actions in and through the IE. Throughout the competition continuum, the JFC integrates OIE into joint plans and synchronizes it with other operations to create desired behaviors, reinforce or increase combat power, and gain decisive advantage. OIE are conducted as an integral part of all operations and campaigns at any level of conflict and help shape the IE. As such, joint forces will always be conducting one or more OIE to remain continuously engaged in and through the IE. The joint force should still integrate information into strategic art and

operational design, planning guidance, and planning processes.

Organizing for OIE

OIE units consist of a headquarters organization with command and control of assigned and attached information forces. JFCs may choose to create a task force for the integrated employment of the specialized capabilities required to conduct OIE.

Information forces are those Active Component and Reserve Component forces specifically organized, trained, and equipped to create and/or support the creation of effects on the IE. Information forces aggregate military personnel, weapon systems, equipment, and necessary support that provide expertise and specialized capabilities that leverage information and conduct activities central to OIE. OIE units are typically composed of the following types of information forces:

- **Psychological Operations Forces.** Psychological operations forces conduct military information support operations, planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the JFC's objectives.
- **Civil Affairs (CA).** CA forces conduct civil reconnaissance, network analysis, and network engagement to support, influence, compel, or leverage populations, governments, and other institutions to expose malign influence, counter coercion and subversion, and impose costs through conventional and unconventional activities.
- **Public Affairs (PA) Organizations.** PA organizations and personnel focus on the OIE core activity of informing domestic, international, and internal audiences.
- **Electromagnetic Spectrum Operations (EMSO) Elements.** EMSO elements assigned to OIE units work with the joint electromagnetic spectrum operations cell at the parent command to organize, execute, and oversee the conduct of electromagnetic warfare and spectrum management.

- **Cyberspace Forces.** Units of the Cyber Mission Force include cyberspace protection teams that defend blue cyberspace in reinforcement to the system operators and local defenders; national mission teams, supported by national support teams, that defend the nation from threats in cyberspace by operating in gray and red cyberspace; and combat mission teams, supported by combat support teams, that project power in support of combatant commander objectives, by operating in and through gray and red cyberspace.
- **Space Operations Elements.** United States Space Force Guardians assigned as planners on OIE unit staffs ensure commanders and their staffs have a common understanding of space operations, provide space domain awareness, and coordinate space capabilities for OIE.

***OIE: Planning,
Coordination, Execution,
and Assessment***

JFCs integrate OIE into operations, as main or supporting efforts, or conduct an OIE as a stand-alone effort. During plan development, the JFC provides planning guidance that describes the desired conditions that must exist in the IE to support mission accomplishment, how the joint force will leverage the inherent informational aspects of its activities to support the JFC's objectives, and the types and level risk that the JFC will accept in the IE. Specifically, for OIE units, the JFC provides guidance on how OIE will support the JFC's scheme of maneuver.

CONCLUSION

This publication provides fundamental principles and guidance to plan, coordinate, execute, and assess the use and leveraging of information during joint operations.

Intentionally Blank

CHAPTER I

FUNDAMENTALS OF INFORMATION

“Information is such a powerful tool that it is recognized as an instrument of national power. The elevation of Information as a joint function impacts all operations. It signals a fundamental appreciation for the military role of information at the strategic, operational, and tactical levels within today's complex operating environment.”

Secretary of Defense James N. Mattis
15 September 2017, *Information as a Joint Function*

1. Overview

a. This joint publication (JP) guides how the joint force considers and uses information to support achieving its objectives. This JP identifies the operational significance of information in achieving commanders' objectives across the competition continuum. This publication is the result of a change in mindset based on the joint force's recognition that all activities have inherent informational aspects that impact the operational environment (OE) and can generate effects that may contribute to or hinder achieving commanders' objectives. The Department of Defense (DOD), in coordination with the other United States Government (USG) departments and agencies, supports the informational instrument of national power by using information to impact the way in which humans and systems behave or function. The joint force leverages information across the competition continuum to assure, deter, compel, and force relevant actor behaviors that support United States (US) interests.

b. The Armed Forces of the United States are poised to fight and win the nation's wars. Transregional, all-domain, and multifunctional threats require the joint force to conduct operations across the competition continuum to prevent armed conflict and set the conditions to prevail during armed conflict. To deter or defeat these threats and achieve strategic objectives, the joint force commander (JFC) should understand how information impacts the OE, use information to support human and automated decision making, and leverage information through offensive and defensive actions to affect behavior. Relevant actors include individuals, groups, populations, or automated systems whose capabilities or behaviors can affect the success of a particular campaign, operation, or tactical action.

c. The joint force can win tactical fights during armed conflict but has not always been able to translate victories into enemy behaviors that lead to intended, enduring, strategic outcomes. Defeat of an enemy, by whatever mechanism, is usually a psychological outcome. The enemy is not really defeated until they believe they are defeated. Even in operations without an enemy or adversary, such as foreign humanitarian assistance, successful outcomes hinge on the perceptions, attitudes, beliefs, and other drivers of behaviors of the affected population.

d. The joint force cannot rely on attrition or its ability to compel behavior through the use of destructive and disruptive lethal force. To support achieving the commander's objectives, the joint force deliberately leverages information through activities that inform

audiences; influence foreign relevant actors; and attack and exploit information, information networks, and information systems.

e. JFCs use the seven joint functions (command and control [C2], information, intelligence, fires, movement and maneuver, protection, and sustainment) in combination to integrate, synchronize, and execute joint operations. The information joint function organizes the tasks required for the management and application of information during all activities and operations. The three tasks of the information joint function stress the requirement to incorporate information as a foundational element during the planning and conduct of all operations. Those tasks are:

- (1) Understand how information impacts the OE.
- (2) Support human and automated decision making.
- (3) Leverage information.

2. The Security Environment

a. The security environment is the set of conditions, circumstances, and influences that affect the employment of the Armed Forces of the United States. It is impacted by advances in information technology (IT) that enable individuals and organizations to access, use, and share information across the globe; to interfere, alter, or disrupt the transmission of information; and to employ and deny information to affect individuals, groups, and automated systems worldwide. Most competitors and adversaries impose some level of restrictions on their populations' access to information or information sources.

b. A defining feature of the security environment is how competitors, adversaries, and enemies are using information as they seek to gain relative advantage over the United States, its allies, and partners and use that advantage to affect behavior and achieve their objectives. Competitors and adversaries rely on enduring campaigns of influence to achieve their objectives and operate below the threshold of armed conflict.

c. Individuals and groups can easily and inexpensively wield information to affect audiences far beyond their physical reach. Technological advances have made IT readily available to individuals and organizations throughout the world and accelerated the increase in global human-to-human, human-to-computer, and computer-to-computer interactions. This has enabled an exponential growth in the amount of information created, processed, and shared. It is now possible for people and automated systems to access information and to instantly communicate globally.

d. Information is pervasive and difficult to control. Populations, organizations, and individuals are capable of sensing, creating, transforming, and disseminating information globally to spread ideas, allowing them to gain momentum and mobilize others to action, even if the information is insufficient, inaccurate, or biased. The proliferation of media

platforms tailored to specific points of view impacts the ability of the joint force to influence relevant actors. This fragmented media environment means that anyone trying to convey information must compete with others for relevance and credibility. The ability to reach and influence audiences requires not just access but an understanding of the factors that affect how they receive, interpret, and act on information.

e. Today, more individuals, organizations, and even automated systems can observe joint force activities, interpret them, and share their observations and interpretations about those activities. These actors use information to affect joint force operations and the joint force's use of information. Competitors, ranging from great powers to non-state actors, use information to avoid or offset the physical overmatch of the United States.

f. State and non-state actors use narratives to shape perceptions and beliefs of audiences. Narratives express ideologies, policies, and strategies and are used to gain or deny popular support. Narratives communicate grievances, goals, and justifications for actions to both internal and external audiences. An effective narrative can induce long-term effects on an audience's beliefs, attitudes, and behavior. A struggle or clash between competing narratives is often referred to as a "battle of the narrative." See Chapter II, "Joint Force Uses of Information," and Chapter IV, "Operational Design and Planning," for a discussion of the joint force's use of narratives. Refer to Appendix A, "Narrative Development," for the seven-step process for developing a narrative.

g. Technological advances and the ease with which people and automated systems can access and use information contribute to today's threats becoming increasingly transregional, all-domain, and multifunctional. Transregional threats are capable of exploiting and using information globally to spur multiple, simultaneous, interconnected crises or conflicts that span more than one combatant command's (CCMD's) area of responsibility (AOR) or functional area. All-domain threats have access to advanced capabilities and exploit IT during operations across all of the physical domains and the information environment (IE) to contest US advantages. Adversaries seek to deter US and combined forces with the threat of sophisticated antiaccess and area denial capabilities that would impose significant losses on friendly forces. Threats employ a broad range of forces

USE OF INFORMATION: RUSSIAN ACTIVITIES IN UKRAINE

Following the admission of Estonia, Latvia, and Lithuania to the North Atlantic Treaty Organization (NATO) in 2004, Russia embarked on a national and military strategy designed to realize regional and global ambitions. This strategy prioritized the reestablishment and maintenance of influence in Russia's "near abroad" and the protection of individual Russians living in those areas. The strategy included the use of "soft power" to exploit the Russian cultural influence and diaspora across its near abroad and especially in the Baltics, Georgia, and Ukraine. Since that time, Russia has employed "information confrontation" to manipulate perceptions and drive behavior with activities that include control of the flow and content of information and the use of disinformation, agents of influence, bribery, staged acts, front organizations, malicious cyberspace activity, and propaganda.

In November 2013, a wave of civil unrest, dubbed “Euromaidan,” began in Maidan Nezalezhnosti, or “Independence Square,” in Kyiv. The protests were in response to Ukrainian President Viktor Yanukovych’s rejection of integration into the European Union in favor of closer ties to Russia. Popular protests and civil unrest continued for several months culminating with violence and the ousting of President Yanukovych. A pro-Western interim government was established, and the situation was seen as a great loss to Russia’s influence in the region. The resulting combination of fleeing pro-Russian officials and the establishment of the interim government in Kyiv created a lapse in governance, providing Russia the opportunity to invade neighboring Ukraine to take control of significant territories and populations, similar to what they had done six years earlier in Georgia.

Russian activities prior and subsequent to the invasion and annexation of Crimea included:

- Providing overt and covert support to Crimean separatists: separatist elements carefully cultivated an image as polite protectors of the Crimean population and encouraged the ethnic Russian majority’s desire for autonomy. Covert Russian agents fomented unrest, undermined the Ukrainian government in Crimea, overwhelmed pro-Ukrainian security forces, and backed local Crimean separatists as they occupied key government buildings, facilitating the isolation of the Crimean peninsula.
- Manipulating and controlling the flow and content of information: The Russians removed all non-Russian radio and television stations in Crimea and cut the underwater communications cable carrying international data to and from the peninsula. Russia dominated the media with disinformation, propaganda, and patriotic themes to “legitimize” Crimea’s call for independence and its eventual annexation. Meanwhile, Russia and its local supporters blocked, intercepted, and manipulated pro-Ukrainian media so there was no effective alternative to the Russian ethno-sectarian narrative.
- Promoting a Russian nationalist narrative in the region and around the world: Russia intensified its ethno-sectarian narrative while its propaganda characterized pro-Ukrainian forces as Nazis and NATO as a threat. In Ukraine, Russia disrupted communications, to include access to the Internet and other media, inhibiting the Ukrainian response to separatist operations.

Various Sources

and systems in an integrated manner to conduct operations that challenge the joint force, most often below the threshold of armed conflict.

3. Information

Information is data in context to which a receiver assigns meaning. Receivers include humans and automated systems and each may acquire information in a variety of

ways (e.g., through spoken or written words, observation, or some other sensing mechanism). Regardless of how they acquire information, a receiver may not be the intended recipient of that information.

a. Humans use information to understand, make decisions, and communicate. Automated systems use information to support decision making, control their own functions, or control the behavior or functions of other systems. Humans and automated systems share information to establish a common understanding and to inform, influence, or direct the behavior of others.

b. By definition, meaning is receiver-centric in that humans and automated systems assign meaning and relevance to the information they receive. The meaning of information that leads to understanding, decision making, and communication relies on both the information itself (data and its context) and factors that influence how a receiver interprets that information. The premise of receiver-centric meaning is that each individual or automated system interprets symbols, messages, and actions differently. To increase the likelihood of a receiver interpreting the information in the way it was intended, the sender considers the factors that influence how a receiver assigns meaning.

(1) The phrase “inherent informational aspects” refers to the features and details of a situation or an activity that can be observed. They are used to derive meaning from that situation or activity. Inherent informational aspects include, but are not limited to, physical attributes of the capabilities and forces involved; the duration, location, and timing of the situation or activity; and any other characteristics that convey information to an observer. Inherent informational aspects, along with the context within which the activity occurs (i.e., the background, setting, or surroundings), are processed through an individual’s worldview to make sense of what is happening. In automated systems, programming and algorithms take the place of worldview. Inherent informational aspects are similar to nonverbal communication; they are the “body language” of activities (see Figure I-1).

The meaning derived by a receiver may be different from what was intended by a sender. For example, transiting United States Navy ships or an amphibious ready group near a coast to demonstrate freedom of navigation (intended meaning) might be interpreted by a foreign government (the receiver) as an indication of an impending invasion (the assigned meaning).

(2) How an observer interprets information to make sense of a situation or activity is influenced by a multitude of factors.

(a) **Human Factors.** A range of complex factors combine to affect how individuals and groups interpret information and make decisions. We refer to these factors as drivers of human behavior because, ultimately, they affect how humans act on information. Attitudes, culture, narratives, and perceptions are detailed here, but any combination of the items summarized in Figure I-2 can drive human behavior.

Examples of Inherent Informational Aspects

Duration:

The time period during which an activity or situation lasts.

Example: Whether an exercise takes place for one day or two weeks. Whether a ship is visible from shore for an hour or for multiple days.

Location:

A position or site in which the activity or situation takes place usually marked by a distinguishing feature.

Example: Whether the situation or activity takes place at a strategic choke point. Whether the situation or activity takes place at or near a religious or culturally significant site.

Timing:

The precise moment or the range of time(s) in which the activity or situation takes place.

Example: Whether a bomber flyover occurred on a significant holiday. Whether raids are conducted during the day or at night.

Platform:

The equipment or capability used during an activity or situation.

Example: Whether a hospital ship or an aircraft carrier is used during a relief mission. Whether US forces are patrolling unilaterally or in conjunction with host nation or multinational partners.

Size:

The physical magnitude, extent, or bulk; relative or proportionate dimensions of the force being presented.

Example: Whether the military presence consists of a seven-person detachment or an infantry company of over 100 people.

Posture:

The state or condition at a given time in particular circumstance; the position or bearing of the force.

Example: Whether or not members of a patrol are wearing individual body armor. Whether flight operations at a base are routine or are modified in response to a change in threat level.

Figure I-1. Examples of Inherent Informational Aspects

1. Attitudes. How humans feel about information impacts how they interpret and remember information. Humans pay greater attention to messages that are consistent with their attitudes and beliefs and tend to discount messages that are

Examples of Drivers of Human Behavior

- **Attitude** is a positive or negative evaluation of a thing based on thoughts, behavior, and social context.
- **Cognition** is the mental process such as thinking, retrieving stored information, and processing of the information. It is the process by which knowledge and understanding is developed in the mind.
- **Culture** is the customs, arts, social institutions, and achievements of a particular nation, people, or other social group.
- **Desire** is a strong feeling of wanting to have something or wishing for something to happen, and may be derived from factors such as affiliation, self-esteem, safety, security, freedom, or power.
- **Emotion** is an internal, conscious mental reaction subjectively experienced and often manifested in physiological reactions and behavior. Emotional appeals are highly effective because they bypass logic and critical thinking.
- **Instinct** is an innate, typically fixed, pattern of behavior derived from events such as will to live, procreation, and pleasure.
- **Language** enables a population/group to interpret or make sense of data and information. Awareness of the attributes of a culture's language can provide insight to a culture's norms, attitudes, and beliefs.
- **Memory** is the store of things learned and retained from activities and experiences. False and inaccurate memories have been shown to affect behavior just as much as accurate ones.
- **Narrative** is a way of presenting or understanding a situation or series of events that reflects and promotes a particular point of view or set of values.
- **Perception** is the organization, identification, and interpretation of sensory information influenced by factors such as experiences, information, education, faith, values, and biases.

Figure I-2. Examples of Drivers of Human Behavior

inconsistent with existing beliefs unless the message is extremely compelling. This cognitive bias causes humans to interpret information so it is consistent with their attitudes and beliefs. Since people tend to remember information that is important to them, this bias impacts how they interpret that information later. This can be helpful as a mental shortcut when trying to make a decision or judgment with a limited amount of information but can also lead to wrong conclusions if individuals have consumed targeted misinformation and propaganda.

2. Culture. Culture significantly influences how humans interpret information, make decisions, and behave. Culture incorporates knowledge, experience, beliefs, values, attitudes, meanings, social hierarchies, religion, notions of time, roles (including sex and age-related roles), and spatial relationships. Sociocultural analysis requires subject matter expertise on the culture and how that culture influences behavior.

3. Narratives. Humans use stories and anecdotal evidence to help them derive meaning from their environment and experiences. Humans combine stories into narratives that they use to describe their version of the past and vision of the future and communicate that vision to others. A narrative can connect seemingly unrelated events and provides an overarching concept that influences thought, meaning, and decision making. Narratives evolve over time. A good narrative will use a range of stories that illustrate, animate, and validate its message. A good narrative will give meaning to a broader vision of how the world should and could be and why an audience should move in the direction of that vision. Humans perceive narratives as credible if they build on their understanding of the world and their social environment to connect new information to the information they already have. Effectively using narratives can shape behaviors and even transform culture. See Chapter II, “Joint Force Uses of Information,” and Chapter IV, “Operational Design and Planning,” for a discussion of the joint force’s use of narratives.

4. Perceptions. Humans derive meaning based upon their perception of the credibility of information and its source. Perceptions rely on reasoning and emotional appeal. Information that elicits an emotional response or confirms a personal bias grabs an observer’s attention and is often perceived as more credible.

(b) Automated Systems. Automated systems are a combination of software and hardware designed and programmed to work automatically without the need for a human operator. Automated systems assign meaning to information in ways that are less complex than those of humans. Humans use information that has been processed by automated systems to support decision making; to establish understanding between each other; and to inform, influence, or otherwise direct the behavior of others. Humans also use automated systems, such as computer algorithms, to control the information an individual or group receives as a means to inform, influence, or direct behavior. Because they are not influenced by emotion or perception, these systems can quickly sort through volumes of information, which would overload human decision makers, and provide a concise analysis or take an action.

c. The receiver determines the relevance and value of information. Information is relevant and valuable when it contributes to understanding the environment, making decisions, performing assessments, or communicating. Information has the most relevance when the receiver perceives it as accurate and timely, and leads to an increase in understanding and a decrease in uncertainty.

d. Information can affect behavior. Understanding the factors that drive behaviors is essential to the effective use of information. One can use information to affect drivers of behavior for automated systems by changing the algorithms, programs, and data that control the system’s behavior (e.g., computer virus) or by sending information to the system’s sensors to produce a predictable output (e.g., jamming a radar). Information can also affect human behavior. This is frequently more complicated because the drivers of behavior do not work in isolation—affecting any one driver can affect other drivers. For example, eliciting strong emotions through an inflammatory headline will affect whether

or not an individual will read the article, but it will also affect how that individual perceives the information contained within the article, regardless of whether it was read.

JOINT FORCE TRANSITION FROM INFORMATION OPERATIONS TO OPERATIONS IN THE INFORMATION ENVIRONMENT

The establishment of the information joint function and the development of this joint publication (JP) on information in joint operations is driving changes across joint and Service DOTMLPF-P [doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy]. One significant doctrinal change is the transition from joint information operations (IO) to operations in the information environment (OIE). This transition is a substantial force development challenge requiring the joint force to evaluate how to organize forces and staffs to deliberately plan and execute OIE.

This publication cancels JP 3-13, *Information Operations*. Joint IO, as defined and practiced, had shortcomings that inhibited it from contributing to the commander's application of informational power. As defined, IO focused on the integration of information-related capabilities (IRCs) to affect the decision making of adversaries and potential adversaries, and effectively ignored other relevant actors that shape the strategic and operational environments. IO planning concentrated on the employment of those IRCs in support of broader joint force operations, ignoring planning for the inherent informational aspects of all activities.

This publication describes how the joint force applies informational power across the competition continuum. That application of informational power includes both the deliberate leveraging of the inherent informational aspects of activities as an imperative for all joint force operations, and the conduct of OIE. OIE are military actions involving the integrated employment of multiple information forces to affect drivers of behavior by: informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems. As such, OIE are distinct from, but complementary to, the joint forces' deliberate leveraging of the inherent informational aspects of military activities during all operations.

OIE calls for formations with the capabilities (i.e., the authorities and tools, as well as subject matter experts possessing in-depth skills, knowledge, and abilities to employ those tools) required to carry out actions that leverage information to affect behavior. Building and resourcing organizations with subject matter experts and tools is part of the joint and Service force development challenge. The joint force and the Services' force development proponents will need to evaluate options to create these organizations and efficiently and effectively ensure that they are manned, trained, and equipped to conduct OIE.

Various Sources

Intentionally Blank

CHAPTER II

JOINT FORCE USES OF INFORMATION

“[The] DOD [Department of Defense] must evolve from a primary focus on executing its preferred method of warfare to one that incorporates information as a foundational element of plans and operations.”

Dr. Mark T. Esper
Secretary of Defense

Written Response to Secretary of Defense Senate Confirmation Hearing
July 2019

1. Military Operations and Information

Information is a resource of the informational instrument of national power at the strategic level. Information is also a critical military resource. The joint force uses information to perform many simultaneous and integrated activities. The joint force uses information to improve understanding, decision making, and communication. Commanders use information to visualize and understand the OE and direct and coordinate actions. The joint force leverages information to affect the perceptions, attitudes, decision making, and behavior of relevant actors. The joint force employment of information is of central importance because it may provide an operational advantage.

2. The Operational Environment and the Information Environment

a. An OE is the aggregated conditions, circumstances, and influences that affect the employment of forces and bear on the decisions of a commander. Each commander’s OE is different from every other commander’s OE.

(1) Within the OE, there exist factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information. We refer to the aggregate of social, cultural, linguistic, psychological, technical, and physical factors as the IE.

(2) The IE is not distinct from any OE. It is an intellectual framework to help identify, understand, and describe how those often-intangible factors may affect the employment of forces and bear on the decisions of the commander.

b. The joint force plans and conducts activities and operations that have inherent informational aspects that will impact the factors that make up the IE. The joint force must account for those informational aspects so that joint force activities and operations affect the OE in a way that supports the JFC’s objectives. Additionally, to ensure unity of effort among different commands, each JFC must consider and communicate how the informational aspects of their planned activities and operations may impact the factors that make up the IE to affect other OEs.

3. Information Advantage

Information advantage is the operational advantage gained through the joint force's use of information for decision making and its ability to leverage information to create effects on the IE. Commanders achieve this advantage in several ways: identifying threats, vulnerabilities, and opportunities along with understanding how to affect relevant actor behavior; obtaining timely, accurate, and relevant information with an ascribed level of confidence or certainty for decision making and the impact of decision making; influencing, disrupting, or degrading the opponent's decision making; protecting the joint force's morale and will; and degrading the morale and will of adversaries. The joint force exploits these advantages through the conduct of operations. For example, disabling an opponent's space-based assets might provide the joint force with the operational advantage of being able to communicate securely over long distances without interruption and of being able to move without being detected. The joint force could then exploit that advantage through an operation to destroy an enemy ground force. Likewise, gaining and maintaining sufficient goodwill among a local population provides the operational advantage of joint forces being able to move more freely in the vicinity of the populace without the locals alerting insurgents to friendly force activities. The joint force could exploit that advantage by conducting operations to capture insurgents hiding in or near civilian populations and by conducting operations that facilitate the host nation (HN) delivery of services to the population.

4. Informational Power

a. Informational power is the ability to use information to support achievement of objectives and gain an informational advantage. The essence of informational power is the ability to exert one's will through the projection, exploitation, denial, and preservation of information in pursuit of objectives. The joint force cannot achieve all of its strategic objectives by relying solely on attrition to coerce change in the behavior of an enemy or adversary. The joint force leverages the power of information as a means to support achievement of its objectives.

b. The joint force applies informational power in two ways. First, the entire joint force plans and conducts all operations, activities, and investments to deliberately leverage their inherent informational aspects. Second, specially trained and equipped units conduct operations in the information environment (OIE). Leveraging the inherent informational aspects of activities in combination with OIE maximizes the effectiveness of all joint force activities.

c. The joint force can leverage the power of information to effectively expand the commander's range of options. The joint force applies informational power:

(1) **To operate in situations where the use of destructive or disruptive physical force is not authorized or is not an appropriate course of action (COA).** The majority of joint force operations support campaigns and do not involve armed conflict. Leveraging information through operations that do not use destructive or disruptive force

may be the only viable option to achieve the JFC's intent and objectives. Conducting noncombat operations and activities to communicate the purpose of joint operations, reinforced by information activities, may be the most effective way for the JFC to develop local and regional situational awareness; build networks and relationships with partners; shape the OE; keep tensions between nations or groups below the threshold of armed conflict; and maintain, enhance, and expand US global influence.

(2) To degrade, disrupt, and destroy the C2 ability of an adversary or enemy. The joint force interferes with an adversary or enemy's ability to execute the decision cycle, thus degrading their ability to make appropriate command decisions. This includes targeting intelligence, surveillance, and reconnaissance (ISR) and C2 systems to interfere with an enemy's ability to understand joint force operations and effectively control their forces.

(3) To prevent, counter, and mitigate the effects of external actors' actions on friendly capabilities and activities. The joint force also uses information for defensive purposes. This includes denying an adversary or enemy access to friendly critical information that would allow them to impede joint force C2, understanding of the OE, movement and maneuver, and sustainment.

(4) To create and enhance the psychological effects of destructive or disruptive physical force. The use of destructive or disruptive force creates psychological effects. Executing actions specifically to create desired psychological effects can elicit profound changes in behavior. Amplifying or manipulating certain features and details of these activities to emphasize the psychological effects of destructive or disruptive force can be a more effective way of achieving joint force objectives than relying on physical force alone to destroy or disrupt enemy capabilities.

(5) To create psychological effects without destructive or disruptive force. The joint force conducts information activities to influence foreign relevant actors, in conjunction with other efforts (e.g., show of force, foreign military sales). In some of these activities, information is the main effort, supported by maneuver elements and the implicit threat of force.

(6) To confuse, manipulate, or deceive an adversary or enemy to create an advantage or degrade the adversary or enemy's existing advantage. By leveraging information to confuse, manipulate, or deceive an adversary, the joint force has the potential to deter threats or induce actions favorable to the JFC. By doing so, the joint force may mislead adversary commanders as to the strength, readiness, locations, and intended missions of friendly forces, causing them to misallocate or waste combat power.

(7) To prevent, avoid, or mitigate any undesired psychological effects of operations. This is particularly true in cases where civilians may be affected by armed conflict. This includes the potential consequences of physical harm, as well as the destruction of homes and key infrastructure. The joint force takes feasible precautions to protect civilians from harm and addresses civilian casualty incidents if they occur. These

efforts include disseminating information to remove civilians from areas of risk, preparing deliberate public communication efforts to minimize reaction to the occurrence of any civilian casualties due to joint force operations, and providing releasable information on actions taken to minimize harm to civilians. More broadly, communication with the civilian population can allay their concerns during periods of increased tension or counter adversary efforts to stoke civil unrest.

INTERMEDIATE FORCE CAPABILITIES

Civilian casualties adversely impact mission accomplishment. After United States Central Command developed formal nonlethal weapons training requirements, there was a 50 percent reduction in civilian casualties between 2011 and 2014. Continued emphasis of United States' use of intermediate force capabilities to reduce civilian casualties demonstrates United States commitment to protection of civilian life and property.

Various Sources

Current and future nonlethal weapons, devices, and munitions will provide the “intermediate force” that can fill the gap between mere presence and lethal effects. Nonlethal weapons are, therefore, more accurately and appropriately characterized as “intermediate force capabilities.” Intermediate force capabilities provide options in situations where individuals may appear to be demonstrating hostile intent, but, in reality, their intentions are innocent rather than true hostile intent. Intermediate force capabilities, when employed in those circumstances, may provide time to better assess intent. They can be appropriate, proportional responses to acts that present hostile intent but fall short of acts or behaviors justifying the use of deadly force. In comparison to lethal weapons, intermediate force capabilities may reduce claims of excessive force, and might be a better option in tactical situations with significant operational, political, or moral equities. Modern intermediate force capabilities are useful beyond law enforcement, security missions, and crowd control. While campaigning through the competition continuum, intermediate force capabilities can address threats with proportional force, and potentially minimize civilian casualties.

US Department of Defense Nonlethal Weapons Program, Executive Agent's Planning Guidance 2020, *Intermediate Force Capabilities: Bridging the Gap Between Presence and Lethality*

(8) To communicate and reinforce the intent of joint force operations, regardless of whether those activities are constructive or destructive. The JFC cannot assume audiences intuitively understand the intent of joint force operations and activities and behave in ways that support the JFC's objectives. Even when the joint force is engaged in constructive activities, audiences may misinterpret the JFC's intent. Planning activities to leverage information based upon an understanding of the intended and likely audiences

will reduce the chance of misinterpretation. In some cases, competitors, adversaries, or enemies will attempt to use disinformation about the intent of joint force activities to undermine joint force credibility and freedom of action or even take credit for the positive outcome of US activities. Planning and conducting joint activities and operations in ways that communicate the intent, supported by OIE, promotes understanding of the mission, enables initiative, and counters disinformation.

(9) **To prepare and support resilience in partner nations' populations.** The imminent or perceived imminent threat of force can be as psychologically damaging as the use of force. Many partner nations execute programs to instill and ensure resiliency in their populations to guard against the psychological effects of potential physical force, as well as to guard against attempted influence by adversary informational activities.

5. Relevant Actors

Advantages are usually thought of in relation to an opponent. However, the joint force also recognizes that friendly and neutral actors also have the potential to positively or negatively impact the friendly mission. By understanding the importance of all the relevant actors and the relationships between them, the JFC develops operation plans (OPLANs) that effectively leverage information to support achievement of objectives. Those relevant actors that the joint force intends to affect then become audiences for inform tasks, target audiences (TAs) for influence tasks, or targets for joint fires or other action.

a. Relevant actors include individuals, groups, populations, or automated systems whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action. The nature of information and how it impacts the OE will change how relevant an actor may or may not be to the success of joint force activities. Military operations have inherent informational aspects that can negatively or positively impact an actor and, ultimately, change how relevant they are to the joint force.

b. Automated systems are the sets of software and hardware that allow computer systems, network devices, or machines to function without human intervention. These automated systems detect and react to sensory inputs to make sense of their environment, act upon that sense making based upon programming or experience, and receive feedback. These systems can be platform-based (e.g., satellite, robot) or may reside and act entirely in cyberspace (e.g., bots, malicious code). Depending upon purpose and required actions, these systems may have a varying degree of autonomy. Examples include, but are not limited to, autonomous vehicles, integrated air defense systems (IADSs) programmed to operate without constant human intervention, and some cyberspace capabilities.

6. Joint Force Use of Narrative

a. Narratives are an integral part of campaigns, operations, and missions. When two or more organizations' narratives are received by an actor, the narratives can be perceived as either competing or complementing. Competing and parallel narratives exist and are used by a broad range of actors (e.g., partners, allies, competitors, adversaries, enemies) to

gain support for their efforts. The joint force strives to provide a compelling narrative that is integrated into OPLANs and resonates with relevant actors by fitting their frame of reference. An effective and integrated narrative can mitigate, undermine, or otherwise render competing narratives ineffective if it is accompanied by complementary actions.

b. The joint force uses narratives as part of campaigning to support understanding the purpose of military operations, link military activities with the activities of other USG departments and agencies, and reflect policy objectives. It provides an overarching expression of strategy and context to a military campaign, operation, or situation. A narrative provides internal and external audiences with the intended meaning of joint force operations, actions, activities, and investments. An effective narrative affects perceptions and attitudes to complement or compete with other narratives. While the joint force conducts all operations to achieve objectives, the narrative explains why the joint force is carrying out operations so the actions are planned and conducted in a way that complements the narrative and avoids a “say-do gap.” Planning joint force missions to align with the narrative helps the joint force increase the probability that relevant actors will derive the intended meaning from joint force operations. The commander’s intent should include a brief statement of the narrative for the operation. It is important to understand that a narrative is not a “fire and forget” document. Once a narrative is introduced, it will most likely have to be further explained and defended based on audience reaction.

c. Synchronization between multiple JFCs contributes to a persistent and global narrative alignment. Informed joint force mission planning reinforces the narrative and increases the probability that relevant actors derive the intended meaning from joint force operations.

7. The Information Joint Function

The information joint function encompasses the management and application of information to change or maintain perceptions, attitudes, and other drivers of behavior and to support human and automated decision making. The information joint function is the intellectual organization of the tasks required to use information during all operations—understand how information impacts the OE, support human and automated decision making, and leverage information (see Figure II-1). JFCs and their staff perform these tasks during all operations to accomplish their respective missions.

a. **Understand how information impacts the OE.** This task helps the joint force identify threats, vulnerabilities, and opportunities in the IE. It provides a foundation for, and supports the continued refinement of, joint intelligence preparation of the operational environment (JIPOE) products to improve the commander’s decision making during planning, execution, and assessment of operations. There are three steps to understanding how information impacts the OE: analyzing of the informational, physical, and human aspects of the environment; identifying and describing relevant actors; and determining the most likely behaviors of relevant actors. These steps are continuous and iterative because the OE is always changing. Planners use the JIPOE products and inputs from other subject matter experts (SMEs) to understand the interrelationships between the informational,

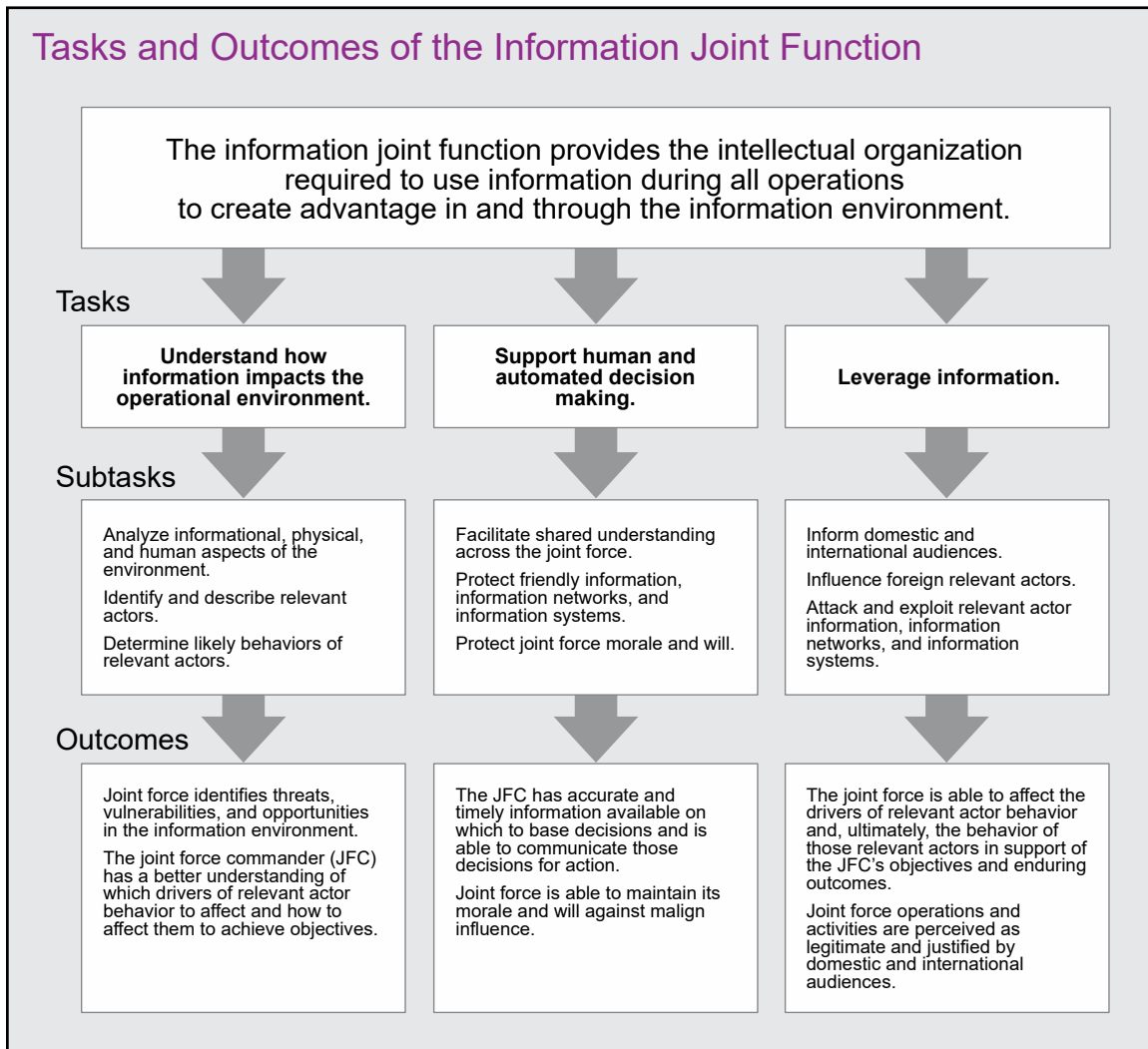


Figure II-1. Tasks and Outcomes of the Information Joint Function

physical, and human aspects within the context of operational objectives. This task requires fusion of multi-source data from across, and external to, the joint force to achieve and maintain an understanding of how information impacts the OE. Sources of internally produced data for this task include inputs from intelligence, public affairs (PA), civil affairs (CA), cyberspace forces, psychological operations units, and C2 systems. Sources of information external to the joint force include USG departments and agencies, businesses, and academic communities, as well as foreign governments, international organizations, nongovernmental organizations (NGOs), and various traditional and nontraditional media sources. This task also relies on language, regional, and cultural expertise to help avoid mirror-imaging and other forms of bias.

For specific planning guidance and procedures regarding language and regional expertise, refer to Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3126.01, Language, Regional Expertise, and Culture (LREC) Capability Identification, Planning, and Sourcing.

(1) **Analysis of the informational, physical, and human aspects of the environment.** Understanding how information impacts the environment and identifying how it can be used to affect behavior requires analysis of the increasingly complex and dynamic relationship of the informational, physical, and human aspects of an environment. A systems approach, such as political, military, economic, social, information, and infrastructure (PMESII), that focuses on the interactive nature and interdependence of each of the aspects to characterize an environment, has been found to be a best practice. Analysis using the three aspects does not separate elements of the environment into “bins” for individual analysis. Instead, this systems approach is a way of describing the different characteristics of objects, activities, or relevant actors; their informational, physical, and human aspects; and the context in which they exist. These results are included in the information staff estimate (see Appendix B, “Information Staff Estimate Format”) and help identify the relevant actors the joint force needs to affect, how to use information to effectively impact those relevant actors, and what friendly information the joint force needs to protect. The running estimate integrates intelligence and other information that characterizes the informational, physical, and human aspects of the environment against the established baseline to identify threats, vulnerabilities, and opportunities.

(a) **Informational aspects** reflect the way that individuals, information systems, and groups communicate and exchange information. Informational aspects are the sensory inputs (e.g., content, medium, format, and context) of activities that a receiver interprets and uses to assign meaning. The content of communication can be verbal and nonverbal. If nonverbal cues do not align with the verbal message, ambiguity is introduced and uncertainty is increased. Medium refers to the system used to communicate (e.g., radio, television, print, Internet, telephone, fax, and billboard). The details of the medium can be described in as little or much detail as necessary. Format is how the information is encoded, such as what language is used, style of delivery (e.g., poetry, songs, imagery), tone, and volume. Context refers to the environment in which the communication happens (e.g., face-to-face, over the phone). Format and context can affect the content of a communication. For example, a text message may contain different content than the same communication delivered face-to-face. Actions are a form of nonverbal communication that have inherent informational aspects and are generally more impactful.

(b) **Physical aspects** are the material characteristics, both natural and manufactured, of the environment that may inhibit or enhance communication. Physical aspects may create constraints and freedoms on the people and information systems that operate in it. Physical aspects are critical elements of group identity and impact how groups form, behave, or might be disrupted or cease to exist. For example, groups may be formed by the people inhabiting an island or an isolated jungle habitat. Similarly, a community might be disrupted by the building of a highway that divides a neighborhood and causes the creation of new, separate, and distinct communities. How information is exchanged is where the interplay between the informational and physical aspects is most apparent. As an example of this interplay, an isolated community without access to modern communications technology will likely have a stronger group identity and be more likely to communicate face-to-face compared to residents of a large modern city.

(c) **Human aspects** are the interactions among and between people and the environment that shape human behavior and decision making. Those interactions are based upon the linguistic, social, cultural, psychological, and physical elements. Human aspects influence how people perceive, process, and act upon information by impacting how the human mind applies meaning to the information it has received. Individuals have distinct patterns of analyzing a situation, exercising judgment, and applying reasoning skills impacted by their beliefs and perceptions. Character and tradition are aspects that suggest how humans perceive a situation and how they might behave under particular circumstances in the future. For example, individual and group identity is often closely related to a geographical area, which can impact how individuals and groups in that region relate to one another and communicate along with the forms that communication may take. Describing these inextricably linked aspects will provide insight into relevant actors' worldviews that frame the perceptions, attitudes, and other elements that drive behaviors.

(2) Identify and Describe Relevant Actors

(a) The analysis of informational, physical, and human aspects of the OE provides the context needed to understand how individuals, groups, populations, and automated systems operate and makes it possible for the joint force to identify who or what is a relevant actor based upon the joint force mission and objectives. The staff conducts this analysis as part of the intelligence directorate of a joint staff (J-2)-led JIPOE process. Equipped with a thorough understanding of its objectives and the general context of the OE, the joint force undertakes deliberate steps to determine the environment in which the relevant actor exists. These efforts include the conduct of intelligence operations and communications with partners to improve knowledge of friendly, neutral, and threat actors and their social, cultural, political, economic, informational, cyberspace, and organizational networks. Intelligence's JIPOE and target systems analysis, psychological operations unit's target audience analysis (TAA), North Atlantic Treaty Organization (NATO) Strategic Communications Division's IE assessment, and CA's area studies and area assessments are analytical products and processes that can help identify and describe relevant actors. Other analysis products may be available from interagency and multinational partners (see Chapter III, "Unity of Effort").

(b) In determining who or what is a relevant actor, the joint force considers the particular function and role of systems, individuals, groups, networks, and populations, while attempting to discern the affiliations and connections among them. Insight into institutions and their processes is often needed to comprehend the roles and relationships among actors. This includes a description of how relevant actors receive information and the factors that will impact the processing and interpretation of that information. The joint force should recognize that mission partners may be relevant actors that need to be understood to ensure unity of effort.

(c) Identifying relevant actors goes beyond just listing entities of the friendly and enemy order of battle. It also includes a range of nonmilitary actors in the environment (e.g., local authorities, civilian supervisory control and data acquisition systems, religious

leaders, community figures). Some potential relevant actors may exist far outside the geographic boundaries of an operation.

(d) This is an iterative process where the staff continuously reassesses the relevance of actors and prioritizes them in regard to the commander's objectives and approach to mission accomplishment. The analysis and description of relevant actors will differ based upon whether the relevant actors are human or automated systems.

(e) When considering relevant actors who are human, gaining an understanding includes multiple inputs from across the staff and from attached units.

1. Describe the relevant actors. Commanders and their staffs describe the individuals, groups, or populations who can aid or hinder success of their missions. As mentioned, some of these may exist outside of the JFC's operational area.

2. Describe what effects the informational, physical, and human aspects of the environment have on each relevant actor; how the actor affects other actors; and the influences the actor has on the environment. This includes identifying what drives joint force and other relevant actor behavior, what narratives are used for their worldview and decision-making processes, and how relevant actors would interpret friendly activities. The JFC needs to understand how the joint force and other relevant actors use information to communicate, so this description should encompass a discussion of each relevant actors' means, context, and patterns of communication.

(f) When considering automated systems, understanding consists of the following two activities:

1. Describe automated systems. Commanders and their staffs should remain aware that, as automated systems become more sophisticated, their behaviors will have greater impact on joint force campaigns, operations, or tactical actions. Automated systems vary based on their degree of autonomy, intelligence, and sophistication. Additionally, their pervasiveness makes it difficult to identify their presence and relevance. Adopting a systems approach as used in JIPOE will help identify automated systems' relevance. Additionally, just as not all human relevant actors are adversaries or enemies of the joint force, or even military in nature, some relevant automated systems will reside outside of the control of adversaries, enemies, and militaries. Understanding automated-systems includes analysis that determines and describes the programming and logic that lead to automated-system decision making and behavior.

2. Describe what effects informational and physical aspects of the environment have on each automated system that is a relevant actor. This includes describing the drivers of behavior and decision-making processes of the automated systems in question. This involves identifying the programming that allows the systems to detect, react to, and learn from the sensory inputs in their environment; act upon that detection based upon programming and experience; and adjust their sensing and actions based upon feedback received. This also involves determining the means, context, and patterns of

automated system communications and how automated systems receive input and communicate decisions and actions, thereby providing the JFC with an understanding of the range of potential behaviors.

(g) As part of JIPOE, network engagement and its associated analyses helps the JFC to identify and understand relevant actors and their associated links with others within a network.

For more information on network engagement, see JP 3-25, Joint Countering Threat Networks.

(3) Identify Likely Behavior of Relevant Actors

(a) This final step builds upon the previous steps to develop a detailed understanding of the range of available behavior options and assess which of those behaviors are most likely to have the greatest impact on the joint force. This is similar to traditional military planning where commanders and their staffs evaluate an enemy's most likely and dangerous COAs.

(b) Identifying the likely behavior of relevant actors also helps the JFC and staff determine which relevant actor COAs in a given time and space will be advantageous or disadvantageous to friendly operations. This leads to the joint force being able to plan for activities that affect the drivers of behavior in support of achieving objectives.

(c) Efforts to anticipate relevant actor reactions and decisions based upon joint force or other actions will be imperfect. Information will frequently be incomplete, imprecise, or flawed. Nevertheless, joint forces make use of the best information available. Once the range of potential behaviors has been determined, the joint force is better able to select appropriate methods to affect future behavior, while considering intended and potential unintended effects. These predictions become inputs to identify initial collection requirements. Once collected and analyzed, the analysis will reveal which COA the relevant actor has adopted.

b. Support human and automated decision making. This task includes facilitating shared understanding across the joint force; protecting friendly information, information networks, and information systems; and protecting joint force morale and will. These activities help ensure the availability of timely, accurate, and relevant information necessary for joint force decision making.

(1) Facilitate Shared Understanding. This task of the information joint function is related to building shared understanding in the C2 joint function and includes collaboration, knowledge management (KM) and information management (IM), and information and intelligence sharing. Although these are typically staff and organizational tasks conducted during daily operations, they are more critical and challenging in today's security environment given the exponential growth in the volume of information the joint force needs to analyze and share. This task requires automated tools that manage and

organize large quantities of disparate, structured, and unstructured data required for decision making. These tools, combined with people and processes, ensure the effective and timely transfer of knowledge to provide an operational advantage to commanders and other decision makers.

(a) **Collaboration.** Collaboration includes activities such as sharing data across the joint force in real time; building situational awareness views; conducting collaborative planning and decision making; execution, coordination, and deconfliction of missions in near real time; and enabling IE visualization. That collaborative environment is enabled by communications systems and applications that improve long-distance, asynchronous collaboration among dispersed forces to enhance planning, execution, and assessment of joint operations. These systems and applications improve efficiency and common understanding during periods of routine interaction among participants and enhance effectiveness during time-compressed operations. Collaboration also requires information and intelligence sharing. Commanders at all levels should determine and provide guidance on what information and intelligence needs to be shared with whom and when. Standard operating procedures should include sharing information to the maximum extent allowed by US law and DOD policy.

(b) **KM and IM.** KM and IM facilitate understanding and decision making. KM is a discipline that integrates people and processes throughout the information lifecycle to create shared understanding, increase organizational performance, and improve decision making. KM identifies and fills knowledge gaps, minimizes or eliminates stovepipes, captures knowledge and transfers it to those who need to know, helps synchronize a battle rhythm, and cultivates a culture of sharing across multiple staff organizations. IM is the function of managing an organization's information resources for the handling of data and information acquired by one or many different systems, individuals, and organizations in a way that optimizes access by all who have a share in that data or a right to that information. IM provides a structure that supports and enables KM. Effective IM contributes to the KM tasks of knowledge creation and supports shared understanding for all unit members. Depending upon the size and mission of the command, the JFC may be supported in their information and KM responsibilities by various staff officers, including chief knowledge and information officers and supporting knowledge and IM officers.

See JP 3-33, Joint Force Headquarters, for additional information on KM and IM.

(c) **Information and Intelligence Sharing.** Sharing of information and intelligence with relevant USG departments and agencies, foreign governments, security forces, interorganizational participants, NGOs, and partner organizations in the private sector promotes interoperability and facilitates collaboration. The joint force shares information to the maximum extent necessary and allowed by US law and DOD policy (e.g., foreign disclosure law and policy). The public affairs officer (PAO), in coordination with the foreign disclosure officer, clears information for public release. While every country has its own sharing caveats, the United States often has additional responsibilities when leading an alliance or coalition. Risk to mission and risk to force related to sharing of information and intelligence is a consideration from the start of operational design in

planning through execution. This includes consideration of the risk of not sharing information and intelligence.

(2) Protect Friendly Information, Information Networks, and Information Systems. This task helps ensure joint force C2 by protecting information and the systems and networks on which it resides from loss, manipulation, or compromise. Protection tasks are conducted during daily activities and are implied, if not specified, tasks for all units during all operations.

(a) Protect Information. The protection of information includes passive and active measures to preserve information and prevent or mitigate competitor, adversary, and enemy collection, manipulation, and destruction of friendly information, to include attempts to undermine the trustworthiness of friendly information. Threats may attempt to manipulate or destroy friendly information to undermine the joint force's understanding, decision making, morale, and will. Activities that contribute to protecting information include intelligence, operations security (OPSEC), military deception (MILDEC), PA, IM, signature management, counterintelligence, cyberspace security procedures, and vulnerability assessments. Two categories of information relevant to joint operations are:

1. Classified information. Classified information is official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure, and which has been so designated. Department of Defense Manual (DODM) 5200.01, *DOD Information Security Program*, identifies the procedures for classifying, marking, downgrading, declassifying, and safeguarding classified information.

2. Critical information. Critical information is specific facts about friendly intentions, capabilities, and activities sought by adversaries and enemies to plan and act so as to thwart friendly mission accomplishment. Critical information may be unclassified information. For example, informational aspects can become signatures that divulge critical information by revealing intent or planned action. Department of Defense Directive (DODD) 5205.02E, *DOD Operations Security (OPSEC) Program*, directs personnel to maintain the essential secrecy of information that is useful to adversaries and potential adversaries to plan, prepare, and conduct military and other operations against the United States. This includes safeguarding critical information from unauthorized access and disclosure.

(b) Protect Information Networks and Information Systems. Adversaries and enemies threaten joint forces through any vulnerability, to include joint force and partner networks, wireless apertures associated with weapons and C2 systems, and other processors and controllers. Through the cyberspace operations (CO) missions of Department of Defense information network (DODIN) operations and defensive cyberspace operations (DCO), cyberspace forces protect the DODIN and, when ordered, other friendly cyberspace capabilities from threats in cyberspace. This activity includes securing the DODIN from known vulnerabilities, educating DODIN users to recognize and thwart malicious cyberspace activity, implementing DOD cybersecurity policy, hunting for

known or suspected threats in blue cyberspace, and engaging threats forward in gray and red cyberspace. These CO are informed by up-to-date knowledge about vulnerabilities in DODIN software and hardware, intelligence about malicious cyberspace activity, and counterintelligence analysis. Protecting the integrity and availability of friendly information helps support decision making.

For additional information on CO, refer to JP 3-12, Joint Cyberspace Operations, and JP 6-0, Joint Communications System.

(3) **Build, Protect, and Sustain Joint Force Morale and Will.** Activities to build joint force morale and will reinforce the baseline strengths the Services have developed in their members to create a cohesive joint force and increase awareness of, and resistance to, malign influence and the demoralizing effects of operations to assure the joint force. Activities to protect joint force morale and will support the force's resiliency against trauma; deployment length; isolation; and propaganda, misinformation, disinformation, deception, persuasion, and dissuasion. As commanders build and protect the forces' resiliency, they prepare to sustain those gains. As conditions change in the OE, the force can be affected in a variety of ways. Sustaining resilience requires commanders to adapt to these changes. Examples of proactive measures and of countermeasures to build, protect, and sustain joint force morale and will include preparing Service members for the psychological effects of loss of life and mitigating those effects when they occur, conducting command information activities, facilitating shared understanding, authenticating trustworthy sources of information, establishing reliable and secure communications, and conducting counter-deception and counter-propaganda activities, as well as conducting religious support and command psychologist activities and facilitating face-to-face communication between command teams and Service members at the lowest echelon. The protection of information, information networks, and information systems task supports the protection of joint force morale by maintaining the integrity of information sent to and received from authenticated and reliable sources. Protecting information contributes to protecting joint force morale and will because it prevents adversaries from accessing or manipulating data and information to incite and spread dissension, confusion, and disorder.

c. **Leverage Information.** When commanders leverage information, they expand their range of options for the employment of military capabilities beyond the use of or threatened use of physical force. JFCs leverage information in two ways. First, by planning and conducting all operations, activities, and investments to deliberately leverage the inherent informational aspects of such actions. Second, by conducting OIE.

(1) **Inform domestic, international, and internal audiences.** Inform activities are the release of accurate and timely information to the public and internal audiences, to foster understanding and support for operational and strategic objectives by putting joint operations in context; facilitating informed perceptions about military operations; and countering misinformation, disinformation, and propaganda. Inform activities help to ensure the trust and confidence of the US population, allies, and partners in US and multinational force (MNF) efforts and to deter and dissuade adversaries and enemies from

action. PA is the primary means the joint force uses to inform; however, civil-military operations (CMO), key leader engagement (KLE), and military information support operations (MISO) also support inform efforts.

(2) **Influence relevant actors.** The purpose of the influence task is to affect the perceptions, attitudes, and other drivers of relevant actor behavior. Regardless of its mission, the joint force considers the likely psychological impact of all operations on relevant actor perceptions, attitudes, and other drivers of behavior. The JFC then plans and conducts every operation to create desired effects that include maintaining or preventing behaviors or inducing changes in behaviors. This may include the deliberate selection and use of specific capabilities for their inherent informational aspects (e.g., strategic bombers); adjustment of the location, timing, duration, scope, scale, and even visibility of an operation (e.g., presence, profile, or posture of the joint force); the use of signature management and MILDEC operations; the employment of a designated force to conduct OIE; and the employment of individual information forces (e.g., CA, psychological operations forces, cyberspace forces, PA, combat camera [COMCAM]) to reinforce the JFC's efforts. US audiences are not targets for military activities intended to influence.

(3) **Attack and exploit information, information networks, and information systems.** The joint force targets information, information networks, and information systems to affect the ability of adversaries and enemies to use information in support of their own objectives. This activity includes manipulating, modifying, or destroying data and information; accessing or collecting adversary or enemy information to support joint force activities or operations; and disrupting the flow of information to gain military advantage. Attacking and exploiting information, information networks, and information systems supports the influence task when it undermines opponents' confidence in the sources of information or the integrity of the information that they rely on for decision making. Activities used to attack and exploit information include offensive cyberspace operations (OCO), electromagnetic warfare (EW), MISO, and CA operations. PA also contributes to this task by publicly exposing malign activities.

8. The Information Joint Function and Joint Operations

The JFC uses the abilities provided by the information joint function during all operations. The **understand task** provides the JFC with the ability to identify threats, vulnerabilities, and opportunities in the IE and provides a better understanding of which drivers of behavior to affect to achieve objectives. These activities facilitate the availability of timely, accurate, and relevant information necessary for joint force decision making. The **leverage task** provides the JFC with the ability to inform audiences; influence foreign relevant actors; and attack and exploit information, information networks, and information systems in support of the JFC's objectives and enduring outcomes. The joint force operationalizes the information joint function through operational design in planning of operations that use information and deliberately leverage the inherent informational aspects of its activities, and by conducting OIE.

a. **Using operational design to plan operations that deliberately leverage the inherent informational aspects of activities and operations.** Everything the joint force does impacts the IE, either by intent or incidentally. All joint force operations, activities, and investments have the potential to affect the perceptions, attitudes, and, ultimately, the behavior of relevant actors. The conclusions that observers draw from interpreting joint force activities may drive them to act in ways that impact the joint force. Whether or not commanders consider this during planning, their activities will impact the IE and resonate in their operational area and potentially other operational areas.

b. **Conducting OIE.** OIE are military actions involving the integrated employment of multiple information forces to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and protecting friendly information, information networks, and information systems. OIE are conducted in support of the JFC's operation or campaign objectives or in support of other components of the joint force. Joint forces continuously conduct OIE to remain engaged with relevant actors. Chapter VII, "Operations in the Information Environment," discusses the conduct of OIE.

CHAPTER III

UNITY OF EFFORT

"At no time in our history has unity among our people been so vital as it is at the present time. Unity of purpose, unity of effort, and unity of spirit are essential to accomplish the task before us."

President Harry S. Truman
Special Message to Congress, 1948

1. Introduction

a. Unity of effort is the coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization. Unified action is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. It is essential to all DOD initiatives to achieve unity of effort through unified action with interagency partners, the broader interorganizational community, and multinational partners. The joint force collaborates with other USG departments and agencies and with multinational partners to effectively use and leverage information to achieve strategic objectives.

b. DOD's role in maintaining unity of effort in and through the IE is, for the most part, the same as it is for the physical domains. DOD establishes policies and sets the conditions for components and their staffs to identify adversarial and potential adversarial threats (including attempts to undermine US alliances and coalitions) and bring capabilities to bear in an effort to affect, undermine, and erode an adversary's or enemy's will. Additionally, DOD closely coordinates operations, activities, and investments with other USG departments and agencies to facilitate horizontal and vertical continuity of strategic themes, messages, and actions.

c. To facilitate unity of effort, the JFC and supporting staff should be familiar with the roles, expertise, and capabilities of individual and organizational stakeholders relative to the use of information and leveraging information to create relative advantage over an opponent. The JFC will need to understand what activities external organizations are currently doing to leverage information and whether the inherent informational aspects of their activities support or hinder the joint force objectives and mission. The JFC's challenge is how best to deconflict, synchronize, coordinate, and/or integrate activities to achieve unified action. This chapter describes the authorities of DOD related to information in joint operations, delineates various roles and responsibilities of organizations that support the joint force use and leveraging of information, describes DOD and interorganizational collaboration and multinational partner considerations regarding their contribution to OIE, and addresses legal considerations in the planning and execution of OIE.

2. Authorities

Military activities that leverage information frequently involve a unique set of complex issues. There are legal and policy requirements, including DOD directives and instructions, national laws, international laws (i.e., international treaties, the law of war), and rules of engagement, all which may affect these activities. Laws, policies, and guidelines become especially critical during peacetime operations and competition when international and domestic laws, treaty provisions, and agreements are more likely to affect planning and execution. Commanders should know who has the execution authority for the conduct of information activities. Many capabilities require separate and distinct execution authorities (e.g., MISO and some CO). Normally, the JFC is designated as the execution authority in the execute order (EXORD) but should consider requests for delegation of certain authorities down to the lower echelons to support tactical commanders. The exercise of operational authority over joint forces conducting information activities inherently requires a detailed and rigorous legal interpretation of authority and/or legality of specific actions. Legal considerations are addressed in more detail later in this chapter. Commanders will also need to know who has release authority for information. For example, release authority can be granted to the joint task force (JTF) PA for unclassified COMCAM products to expedite their release to the media.

a. **Title 10, United States Code (USC)**, outlines the role of the Armed Forces of the United States and provides the legal basis for the roles, missions, and organization of each of the Services as well as DOD. Title 10, USC, Section 164, gives command authority over assigned forces to the combatant commander (CCDR), which provides that individual with the authority to organize and employ commands and forces, assign tasks, designate objectives, and provide authoritative direction over all aspects of military operations. Specifically, Title 10, USC, Chapter 19, authorizes the military to conduct operations, including clandestine operations, in the IE to defend the United States, its allies, and its interests. This includes operations in response to malicious influence activities carried out against the United States or a US person by a foreign power. Authorities for specific types of operations are established within Secretary of Defense (SecDef) policies, including DOD instructions, directives, and memoranda, as well as in EXORDs and operation orders authorized by the President or SecDef and subordinate orders issued by commanders approved to execute the subject missions.

(1) ***The Department of Defense Strategy for Operations in the Information Environment*** established strategic initiatives for DOD to operate effectively in and through the IE, defend national interests, and achieve national security objectives. This strategy guides DOD support to the whole-of-government effort. It complements, and supports, other guidance documents, including the *National Security Strategy of the United States of America, 2017* [short title: NSS]; *2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* [short title: NDS]; *Department of Defense Cyber Strategy 2018*; and the *Department of Defense Strategy for Implementing the Joint Information Environment*, which focuses on IT implementation. In general, the *Department of Defense Strategy for Operations in the Information Environment* describes operational-level objectives for OIE in which, through operations,

actions, and activities in the IE, DOD has the ability to affect the decision making and behavior of adversaries and designated others to gain advantage across the competition continuum.

(2) **The Global Integrated Operations in the Information Environment [short title: GIOIE] EXORD** directs the joint force to conduct globally integrated operations to maximize the cognitive impacts of combined informational power and physical force on an adversary and other relevant actor perceptions and decision making, to coerce behavior, communicate the costs of aggression, offer opportunities for updating alliances, and create new strategic partnerships to protect US interests. The GIOIE EXORD also addresses the need to improve OIE by adopting methods that deliberately align our analysis, decisions, investments, activities, operations, and relationships in time, space, and purpose.

b. **Title 50, USC, Section 3093**, states that any activity of the USG to influence political, economic, or military conditions abroad, where it is intended that the role of the USG will not be apparent or acknowledged publicly, is a covert action and is only authorized pursuant to a Presidential finding. This is considered during the identification of attribution requirements and impacts any non-attribution or delayed attribution decisions. The law further states that traditional military activities fall outside of the statute.

c. **Title 17, USC**, governs the use of copyrights. The joint force uses a variety of multimedia formats and commonly incorporates music, symbols, graphics, and messages into its products. It is important to note these products are required to adhere to the copyright restrictions under Title 17, USC, that protect published and unpublished works in a variety of forms and formats.

3. Responsibilities

Information can have significant regional and global impacts that challenge the joint force with unanticipated threats, vulnerabilities, and opportunities. Effectively dealing with these challenges and communicating intended meanings to selected populations requires individuals and organizations across DOD and interagency partners to ensure coherency with, and align their policies and activities to, national strategic objectives. Unified command enables the synchronization, coordination, and/or integration of activities of governmental and nongovernmental entities with military operations to achieve unity of effort in support of an overall strategy. Senior leaders work with the other members of the national security community to promote unified action. A number of factors can complicate the coordination process, including various agencies' different and sometimes conflicting policies and overlapping legal authorities, roles and responsibilities, procedures, and decision-making processes for information activities. This section describes responsibilities of individuals and organizations related to achieving and maintaining unity of effort in the application of informational power.

a. **The President of the United States.** The President exercises authority over and control of the Armed Forces of the United States. The President frames the strategic context through guidance documents like the NSS, Presidential policy directives, EXORDs, and other national strategic documents, informed by the National Security Council (NSC) and Homeland Security Council. These national strategic documents, provided by the President or NSC, provide strategic guidance that is passed along to military planners and provided to the JFC. The end result should be a military plan that aligns both operations and communications with the national strategy (see Chapter IV, “Operational Design and Planning”).

b. **NSC.** The NSC is the President’s principal forum for considering and deciding national security policy with the President’s senior national security advisors and Cabinet officials. The NSC facilitates the development of an integrated approach to strategic matters, allowing the USG departments and agencies to bring their assets to bear in keeping with statutory roles. SecDef is a statutory member of the NSC and the Chairman of the Joint Chiefs of Staff (CJCS) is the military advisor to the NSC. The NSC provides a forum through which various USG departments and agencies can develop a common understanding of the situation and review and identify the need for policy changes and adjustments. The NSC’s Information Statecraft Policy Coordination Committee is a mechanism for interagency coordination on messaging and influence strategies.

Refer to JP 1, Volume 1, Joint Warfighting, and CJCSI 5715.01, Joint Staff Participation in Interagency Affairs, for more information on the NSC and its membership.

c. **SecDef.** SecDef is the principal assistant to the President for all DOD matters, with authority, direction, and control over the entire DOD. SecDef oversees the development of broad defense policy goals and priorities for the deployment, employment, and sustainment of US military forces based on the NSS. For planning, SecDef provides guidance to ensure that military action supports national objectives through the NDS, *Defense Planning Guidance*, *Contingency Planning Guidance*, *Global Force Management Implementation Guidance*, and the *Department of Defense Strategy for Operations in the Information Environment*. These guidance documents are used by the CJCS to develop the *National Military Strategy* [short title: NMS], which CCDRs translate into clear planning guidance with desired, behaviorally focused objectives. Additionally, SecDef articulates the joint force strategic messages to focus operations within the context of the overarching USG narrative.

(1) **Under Secretary of Defense for Policy (USD[P]).** The USD(P) is the principal advisor to SecDef on the exercise of policy development, planning, resource management, fiscal, and program evaluation responsibilities.

(a) The USD(P) manages DOD-level programs and oversees all activities related to the use and application of information by DOD. In this capacity, the USD(P) manages guidance publications (e.g., DODD 3600.01, *Information Operations [IO]*) and associated policy on behalf of SecDef. The USD(P) is responsible for tasks related to information activities as delineated in DODD 3600.01.

(b) The USD(P) acts as the principal information operations advisor to SecDef and carries out responsibilities as detailed in Title 10, USC, Section 397.

Refer to DODD 5111.01, Under Secretary of Defense for Policy (USD[P]), for more information on the roles and responsibilities of the USD(P).

(c) **Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict (ASD[SO/LIC]).** The ASD(SO/LIC) is the principal civilian advisor to SecDef on special operations and low-intensity conflict matters and has overall supervision (to include oversight of policy and resources) of those operations and activities. In addition to policy oversight for special operations and stabilization capabilities, the ASD(SO/LIC) has policy oversight for strategic capabilities and force transformation and resources. As such, ASD(SO/LIC), after SecDef and the Deputy Secretary of Defense, is the principal official charged with oversight over all special operations and low intensity conflict warfighting capabilities within the senior management of DOD. The ASD(SO/LIC) also has responsibility for policy formulation and implementation related to information-related activities as detailed in DODD 5111.10, *Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict*.

(d) **Assistant Secretary of Defense for Homeland Defense and Global Security (ASD[HD&GS]).** The ASD(HD&GS) develops policy and oversees planning, capability development, and operational implementation for countering weapons of mass destruction, defense continuity, mission assurance, and defense support of civil authorities and supervises homeland defense activities of DOD.

(e) **Assistant Secretary of Defense for Space Policy.** Fills the role of Principal Cyber Advisor and includes the office of **Deputy Assistant Secretary of Defense for Cyber Policy**, who establishes and oversees the implementation of DOD cyberspace-related policy and strategy, integrating it with national cyberspace policy and guidance. Provides guidance and oversight on DOD CO as they relate to foreign cyberspace threats, international cooperation, engagement with foreign partners and international organizations, and implementation of DOD cyberspace strategy and plans, including those related to cyberspace forces and their employment.

Refer to DODD 5111.13, Assistant Secretary of Defense for Homeland Defense and Global Security (ASD[HD&GS]), for more information on the roles and responsibilities of the ASD(HD&GS).

(2) **Assistant to the Secretary of Defense for Public Affairs (ATSD[PA]).** The ATSD(PA) is the principal staff assistant and advisor to SecDef for DOD news media relations, internal communications, community outreach, PA, and audio-visual information. The ATSD(PA) is the sole authority for release of official DOD information, to include, but not limited to, press releases and visual information (VI) materials including COMCAM footage. As the principal spokesperson for DOD, the ATSD(PA) develops communication policies, plans, and programs in support of DOD objectives and operations, along with a wide variety of DOD public outreach activities. ATSD(PA) coordinates with

USD(P) to ensure DOD information activities are consistent with the policy established in DODD 3600.01, *Information Operations (IO)*, and DOD influence activities are not directed at or intended to manipulate US audiences, public actions, or opinions and are conducted in accordance with all applicable US statutes, codes, and laws. ATSD(PA) interfaces with the CCMDs, normally through their joint interagency coordination group (JIACG) and passes information down through public affairs guidance (PAG). The ATSD(PA) publishes PAG ahead of plan execution to provide a common reference for all military and USG organizations. PAG helps the USG present a coherent narrative and includes themes to assist the joint force in deliberately aligning the inherent informational aspects of their activities with those themes.

Refer to DODD 5122.05, Assistant to the Secretary of Defense for Public Affairs (ATSD[PA]), for more information on the roles and responsibilities related to the ATSD(PA).

(3) Under Secretary of Defense for Intelligence and Security (USD[I&S]). The USD(I&S) is the principal staff assistant and advisor to SecDef and the Deputy Secretary of Defense on intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. These matters include coordination of activities within the intelligence community (IC) related to DOD management and application of information, as well as serving as the Office of the Secretary of Defense (OSD) program management lead for the DOD OPSEC and MILDEC programs.

Refer to DODD 5143.01, Under Secretary of Defense for Intelligence and Security (USD[I&S]), for more information on the roles and responsibilities related to the USD(I&S).

(4) Under Secretary of Defense for Acquisition and Sustainment (USD[A&S]). The USD(A&S) is the principal staff element for DOD for acquisitions, advanced technology, and logistics. The USD(A&S) manages the DOD special access program (SAP) management and control structures through the Special Program Directorate and executes proponent responsibilities for EW. The USD(A&S) enables the delivery and sustainment of secure and resilient information capabilities to the warfighter and international partners quickly and cost effectively.

Refer to DODD 5135.02, Under Secretary of Defense for Acquisition and Sustainment (USD[A&S]), for more information on the roles and responsibilities related to USD(A&S).

(5) DOD Chief Information Officer (CIO). The DOD CIO is the principal staff assistant and senior advisor to SecDef and the Deputy Secretary of Defense for IT, information resources management, and efficiencies. The DOD CIO is DOD's primary authority for the policy and oversight of information resources management, to include matters related to IT, network protection, and network operations. The DOD CIO is responsible for all matters relating to the DOD information enterprise, such as cybersecurity policy and standards; communications; information systems; spectrum management; network interoperability policy and standards; positioning, navigation, and

timing policy; and the DOD information enterprise that supports DOD C2. In this capacity, the CIO develops DOD strategy and policy on the operation and protection of all DOD IT and information systems, including development and promulgation of enterprise-wide architecture requirements and technical standards; enforcement, operation, and maintenance of systems, interoperability, collaboration; and interface between DOD and non-DOD systems. The DOD CIO exercises authority, direction, and control over the director of the Defense Information Systems Agency (DISA) and the Joint Artificial Intelligence Center (JAIC).

(a) **DISA.** DISA is a DOD combat support agency that provides, operates, and ensures C2 and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission partners across the full spectrum of military operations. DISA ensures mission partners have secure, available, and reliable services and capabilities to achieve their mission in a contested cyberspace. DISA enhances operations through the security, operation, and defense of the DISA-managed portion of the DODIN, management of the Cyber Security Service Provider program, and support to CCMDs, including United States Cyber Command (USCYBERCOM) and its subordinate Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN).

(b) **JAIC.** The JAIC provides expertise to help the DOD harness the power of artificial intelligence. The JAIC integrates technology development, with the requisite policies, knowledge, processes, and relationships to ensure long-term success and scalability. The JAIC seeks to deliver an information advantage to DOD working to accelerate the delivery and adoption of artificial intelligence to achieve mission impact at scale. The goal is to use artificial intelligence to solve large and complex problem sets that span multiple Services, then ensure the Services and components have real-time access to ever-improving libraries of artificial intelligence data sets and tools.

d. **Department of State (DOS) Organizations.** DOS plans and implements foreign policy. DOS is led by the Secretary of State, who is the President's principal advisor on foreign policy and the person chiefly responsible for US representation abroad. DOS's primary job is to promote and communicate American foreign policy throughout the world. DOS interfaces with representatives of foreign governments, corporations, NGOs, and private individuals. A key DOS function is assembling coalitions to provide military forces for US-led multinational operations, as well as communicating the President's policies to other nations and international bodies. The following internal DOS offices have information-related duties and with whom DOD planners may need to coordinate OIE:

(1) **Under Secretary for Public Diplomacy and Public Affairs.** The Under Secretary for Public Diplomacy and Public Affairs serves as the lead policy maker for DOS's overall public outreach and press strategies. The Under Secretariat team coordinates closely with the regional bureaus, functional bureaus, interagency partners, the private sector, and international partners to ensure DOS's public diplomacy and PA activities are consistent, forward-looking, supportive of US foreign policy, and grounded in research.

(a) **Bureau of Educational and Cultural Affairs.** The Bureau of Educational and Cultural Affairs designs and implements educational, professional, and cultural exchanges and other programs that create and sustain the mutual understanding with other countries necessary to advance US foreign policy goals. The Bureau's programs cultivate people-to-people ties among current and future global leaders that build enduring networks and personal relationships and promote US national security and values sharing America's rich culture of performing and visual arts with international audiences.

(b) **Bureau of Global Public Affairs.** The Bureau of Global Public Affairs serves the American people by effectively communicating US foreign policy priorities and the importance of diplomacy to American audiences and engaging foreign publics to enhance their understanding of and support for the values and policies of the United States. Some of the centers and offices in this bureau include:

1. **Foreign Press Centers.** The Foreign Press Centers' mission is to deepen understanding of US policy and American values through engagement with foreign media. They provide clear and accurate understanding of policy and American values to global audiences via first-hand access. The Foreign Press Centers support US policies by helping foreign media cover the United States and by providing direct access to authoritative American information sources.

2. **Office of Global Social Media.** The Office of Global Social Media expands the reach of US foreign policy through new media and web-based communication technology. Working with the entire DOS, the team maintains the DOS's official blog, DipNote. The office also maintains DOS's official presence on social media platforms.

3. **Office of Global Web Platforms.** The Office of Global Web Platforms oversees the DOS's use of websites to inform the public. State.gov delivers information about DOS, such as press releases, key policy information, and details about the US relationship with countries and areas of the world. Complementing state.gov, the team manages the platform on which nearly 200 missions update their own websites to communicate with local audiences. The team coordinates with all bureaus and offices in DOS and trains both domestic and mission staff to use the Internet to communicate effectively.

4. **Office of International Media Engagement.** The Office of International Media Engagement creates and manages DOS mechanisms to ensure accurate coverage of US foreign policy priorities by major international media. The office oversees the DOS's six regional media hubs, which serve as overseas platforms for engagement of foreign audiences via the media. The office ensures DOS international media capabilities are integrated into the interagency press and PA planning and execution. The office works within the Bureau of Global Public Affairs and with DOS regional bureaus and other USG departments and agencies to develop foreign media engagement strategies in furtherance of US foreign policy priorities.

5. Office of Press Operations. The Office of Press Operations supports the President and Secretary of State by explaining the foreign policy of the United States and the positions of DOS to domestic and foreign journalists. The office responds to press queries, conducts media interviews, monitors media for breaking international events, and coordinates special press briefings and conference calls.

6. Office of Public Liaison. The Office of Public Liaison connects DOS to domestic audiences to advance the DOS's work at home and abroad. The Office of Public Liaison also responds to inquiries on foreign policy issues, handles requests for briefings from groups coming to DOS, and partners with organizations to sponsor major conferences and events.

(c) Global Engagement Center. The Global Engagement Center directs, leads, synchronizes, integrates, and coordinates efforts of the federal government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States and its allies and partner nations. The Global Engagement Center partners with DOD to counter propaganda and disinformation from foreign nations. One initiative supports public and private partners working to expose and counter propaganda and disinformation from foreign nations.

(d) Office of Policy, Planning, and Resources. The Office of Policy, Planning, and Resources for Public Diplomacy and Public Affairs provides long-term strategic planning and performance measurement capability for public diplomacy and PA programs. It also enables the Under Secretary to better advise on the allocation of public diplomacy and PA resources, to focus those resources on the most urgent national security objectives, and provide realistic measurement of public diplomacy's and PA's effectiveness.

(e) US Advisory Commission on Public Diplomacy (ACPD). The ACPD appraises USG activities intended to understand, inform, and influence foreign publics and to increase the understanding of, and support for, these same activities. The ACPD conducts research and symposiums that provide independent assessments and informed discourse on public diplomacy efforts across government. Supported by the Under Secretary of State for Public Diplomacy and Public Affairs, the Commission reports to the President, Secretary of State, and Congress.

(2) Country Teams. The country team unifies the coordination and implementation of US national policy within each foreign country under the direction of the chief of mission (COM), working directly with the HN government, and consists of key members of the US diplomatic mission or embassy. Country teams meet regularly to advise the COM on matters of interest to the United States and review current developments in the country. The COM, as the senior US representative in each HN, controls information release in country. The CCMDs are the primary entry point for DOD personnel to coordinate with country teams in their AOR. CCMD staff coordinates all themes, messages, VI products, and press releases impacting an HN through the respective US embassy channels. The DOS

foreign policy advisor (POLAD) at CCMDs can facilitate access to DOS and has reachback to resources for CCMD staff. The COM also directs the country team system, which provides the means for rapid interagency consultation and action on recommendations from the field (including US embassies, CCMDs with an AOR, and international programs) with a consistent USG voice and effective execution of US programs and policies. The CCDR and staff should establish habitual working relationships with relevant organizations before incidents occur that trigger planning and requests for military resources. As emergent events requiring planning develop, the normal flow of DOS and other agencies reporting from the field will increase significantly. Under the country team construct, USG departments and agencies are required to coordinate their plans and operations (including OIE) and keep one another and the COM informed of their activities (including activities that leverage information). The COM has the right to see all communication to, or from, mission elements, except those specifically exempted by law or executive decision.

e. **The Joint Staff (JS).** The JS assists the CJCS in accomplishing responsibilities for the unified strategic direction of the combatant forces, their operation under unified command, and for their integration across Service components. The direction of the JS rests exclusively with the CJCS. Additionally, the JS coordinates with CCMDs, OSD, and other USG departments and agencies to achieve unity of effort. The following directorates perform functions that directly support the joint force use and leveraging of information:

(1) **CJCS.** A primary statutory responsibility assigned to the CJCS in Title 10, USC, is to act as the principal military advisor to the President, SecDef, and NSC. The CJCS functions under the authority, direction, and control of SecDef; transmits communications between SecDef and CCDRs; and oversees activities of CCDRs, as directed by SecDef. The CJCS develops the NMS, which provides the CJCS's guidance on information and its role in strategy. The CJCS also updates CJCSI 3050.01, *Implementing Global Integration*, and CJCSI 3110.01, *(U) Joint Strategic Campaign Plan (JSCP)* [short title: JSCP], which includes planning direction related to the joint force's leveraging of information. Cross-functional teams (CFTs) facilitate the effort to organize and coordinate operations, actions, and activities in the IE. The JSCP includes guidance mandating that all commanders develop operations and activities with the aim to emphasize informational aspects of those operations and activities. The CJCS represents the Military Departments in national security policy-making activities of the interagency process. In this role, the CJCS assists SecDef in implementing operational responses to global threats and acts as the coordinating authority for transregional threat planning and response. From an information perspective, the CJCS functions as the oversight authority for policy execution within the CCMD and subordinate commands; develops procedures for a professionally trained and educated joint information force in coordination with the Under Secretary for Personnel and Readiness and USD(P); emphasizes the importance of including information as an instrumental part of military operations through the development and validation of joint doctrine; validates information requirements; serves as the joint proponent for MILDEC, OPSEC, PA/VI/COMCAM, and information activities; and ensures coordination and deconfliction of joint information and intelligence activities in all planning and execution.

(2) **Director, Joint Staff (DJS).** The DJS is the primary advisor to the CJCS on the application of informational power and acts as the CJCS's lead for cross-staff, joint force, intra-DOD, and interagency coordination for the management and application of information. The Directorate of Management (DOM) is part of the Office of the DJS. The Director of DOM serves as the DJS's principal advisor on enterprise mission support and management operations. The Director of DOM also acts as the JS's principal planner, director, and representative on all mission support and management matters. The DOM supervises all facility and security operations at 18 locations throughout the continental United States, with special emphasis on those that serve as nodes of the National Military Command System with a staff of civilians, uniformed military, and contractor professionals. The DOM supervises, administers, and integrates all enterprise decision support systems, processes, and procedures to meet DOD and Title 10, USC, requirements for accountability, standardization, execution, and reporting.

(3) **Joint Staff J-2 [Intelligence].** The JS J-2 implements Office of the Under Secretary of Defense for Intelligence and Security policy for intelligence support for the management and application of information in joint operations, including characterization of the IE and intelligence support to OIE. The JS J-2 coordinates with the CCMDs to staff intelligence-related CJCS orders (e.g., alert orders, planning orders, warning orders) and coordinate requests for forces (RFFs) in response to a CCMD request for intelligence capabilities.

(4) **Joint Staff J-3 [Operations]**

(a) **JS J-3 Director.** The JS J-3 Director assists the CJCS in carrying out responsibilities as the principal military advisor to the President and SecDef by developing and providing guidance to the CCDRs and by facilitating communications between the President, SecDef, and the CCDRs regarding current operations and plans.

(b) **Joint Staff J-39 [Deputy Director for Global Operations].** The JS J-39 advises the JS J-3 and CJCS on OIE and special actions. The JS J-39 serves as the JS focal point for OIE and special technical operations (STO), sensitive DOD support to/from non-DOD agencies, MISO, and OCO and DCO.

(5) **Joint Staff J-5 [Strategy, Plans and Policy].** The JS J-5, in coordination with the JS J-2, JS J-3, OSD PA, CJCS PA, Office of the Under Secretary of Defense for Policy, and Office of the Under Secretary of Defense for Intelligence and Security, develops and coordinates globally integrated, campaign-level, thematic information guidance linked to national security direction and national security policy and in support of whole-of-government strategic communications objectives. Additionally, the JS J-5 coordinates on strategic information guidance and plans with the NSC Inter-Agency Policy Committee, the IC, and DOS. This coordination ensures continuous alignment among understanding of the threat, military actions including PA activities, and military contributions to national/interagency communications strategy and communication guidance. The JS J-5 provides planning recommendations and oversight through the joint planning and execution community (JPEC) process to regional, transregional, and country-specific strategy, plans, and policy recommendations, to include the development and

coordination of military information activities. In coordination with the JS J-3, develop assessment criteria for information activities. The JS J-5 also leverages multinational contacts to advise, collaborate, monitor, and report concerning the information efforts of our allies and partners. Under the Promote Cooperation Program, the JS J-5 facilitates periodic interagency working groups that include CCMD planning staffs, other DOD offices, and agency partners for collaboration on planning (e.g., campaign and other contingency plans). The Promote Cooperation Program ensures DOD speaks with one voice and the information shared with other USG departments and agencies is fully vetted and authorized.

(6) Joint Staff J-6 [Command, Control, Communications & Computers/Cyber]. The mission of the JS J-6 is to assist the CJCS in providing the best military advice, while advancing DODIN protection, joint/multinational interoperability, and C2 capabilities required by the joint force to preserve the nation's security. In conjunction with OSD, the JS, and operational stakeholders, JS J-6 facilitates managing requirements for the C2 of the IE program and other requirements that support the management and application of information in joint operations.

(7) Joint Staff J-7 [Joint Force Development]. The JS J-7 is responsible for the six functions of joint force development—doctrine, education, concept development and experimentation, training, exercises, and lessons learned. The JS J-7 supports the CJCS and the joint warfighter through joint force development to advance the operational effectiveness of management and application of information in the current and future joint force. The JS J-7 works with CCMDs to ensure adequate inclusion of informational capabilities and concepts in exercises. In conjunction with the JS J-39 and JS PA, the JS J-7 develops exercise/experiment concept details and workable implementation plans for exercise inclusion, supports exercise development throughout the joint event life cycles, and reports exercise dates and descriptions to facilitate the identification of opportunities and vulnerabilities related to the management and application of information in joint operations.

f. **CCDRs.** The *Unified Command Plan* provides guidance to CCDRs, assigning them missions. CCDRs exercise combatant command (command authority) over assigned forces and are directly responsible to SecDef for the preparedness of their commands to perform, and their performance of, assigned missions. CCDRs are responsible for the implementation of strategy and US policy and the execution of assigned missions. One way they do this is by integrating, synchronizing, and employing forces to achieve effects in the IE that support achievement of operational objectives. CCDRs also translate national strategic objectives into operational objectives that specify the desired behavior of relevant actors to support the attainment of enduring strategic outcomes. CCDRs organize their staffs to best employ the information joint function. This may include standardizing organizational practices by aligning related capabilities into the same directorate, establishing routine working groups, and establishing a center with responsibility for the information joint function tasks, while maintaining PAO as their principal spokesperson, senior advisor, and a member of their personal staff. They also ensure all plans mitigate vulnerabilities, counter threats, and exploit opportunities in the IE. CCDRs develop and

prioritize intelligence requirements that support leveraging information. CCDRs and subordinate JFCs develop, plan, program, and assess information activities during all phases of military engagement across the competition continuum; in coordination with the USD(P) and CJCS, identify and seek the appropriate delegated authorities required for leveraging information; integrate information guidance for theater planning and deliberate and contingency planning; develop interagency coordination requirements and mechanisms for each OPLAN; and ensure coordination and deconfliction of CCMD information and intelligence activities in all operational planning and execution. CCDRs guide the collaborative development of narratives for their assigned responsibilities and ensure actions across AORs or functional areas to align with that narrative. The following CCDRs have additional responsibilities related to the information joint function:

(1) Commander, United States Special Operations Command (CDRUSSOCOM). CDRUSSOCOM is the designated joint proponent for MISO and CA, responsible for leading the collaborative development, coordination, and integration of MISO and CA capabilities across DOD. This responsibility is focused on enhancing interoperability and providing other CCDRs with MISO and CA planning and execution capabilities. CDRUSSOCOM also serves as the coordinating authority for MISO Web Operations, and conducts transregional MISO with concurrence from applicable CCMDs. The United States Special Operations Command Joint MISO Web Operations Center provides the JFC with a capability which facilitates and conducts MISO employing social media, mobile applications, websites, and other Internet-based capabilities and technologies to influence foreign audience behavior.

(2) Commander, United States Cyber Command (CDRUSCYBERCOM). CDRUSCYBERCOM is the coordinating authority for global CO. This responsibility includes planning, coordinating, integrating, synchronizing, and conducting OCO, DCO, and DODIN operations. CDRUSCYBERCOM conducts CO in support of national objectives and provides other CCDRs with CO planning and execution capabilities.

(3) Commander, United States Strategic Command (CDRUSSTRATCOM). CDRUSSTRATCOM's assigned responsibilities include strategic deterrence, nuclear operations, joint electromagnetic spectrum operations (JEMSO), global strike, global missile defense, and analysis and targeting. As the joint proponent for JEMSO, CDRUSSTRATCOM focuses on enhancing interoperability and providing other CCDRs with contingency EW expertise in support of their missions. This is in addition to the responsibilities shared by all CCDRs, in coordination with the USD(P) and through the CJCS. CDRUSSTRATCOM coordinates JEMSO.

(4) Commander, United States Space Command (USSPACECOM). Commander, USSPACECOM, plans and executes global space operations, activities, and missions. Space supports the flow of information and decision making. It may also serve as an information capability essential to the delivery of specific information in the IE. Space control consists of operations to ensure freedom of action in space for the United States and its allies and, when directed, deny an adversary freedom of action in space. The

space control mission area includes defensive and offensive activities; supported by the requisite current and predictive knowledge of the space environment.

(5) Commander, United States Transportation Command (USTRANSCOM). Commander, USTRANSCOM, is responsible for mobility and joint enabling capabilities. One of USTRANSCOM's components is the Joint Enabling Capabilities Command that provides mission-tailored capability packages on short notice for limited duration to assist the joint force plan, prepare, establish, and operate joint force headquarters in globally integrated operations. The Joint Planning Support Element (JPSE) deploys expeditionary, mission-tailored, joint SME across operations, plans, sustainment, intelligence, KM, and PA.

Refer to JP 3-08, Interorganizational Cooperation, for more information on the various organizations and their respective roles and responsibilities related to interorganizational cooperation.

g. **Joint Organizations.** The following joint organizations perform functions that support the joint force use and leveraging of information:

(1) **Joint Information Operations Warfare Center (JIOWC).** The JIOWC is a CJCS-controlled activity under the supervision of the JS Director for Operations. JIOWC enables the application of informational power at the strategic level and performs CJCS proponent responsibilities for joint enterprise information and information activities, MILDEC, and OPSEC, to create, enhance, or protect joint force advantages in the IE. The JIOWC provides OIE subject matter expertise and advice to the JS and CCMDs, facilitates CCMD and Service collaborative efforts to identify and develop joint OIE concepts and solutions, assists in advocating for and integrating CCMD OIE requirements, and assists in developing and coordinating force development requirements for joint force information professionals.

(2) **Joint Planning Support Element-Public Affairs (JPSE-PA).** JPSE-PA, a functional group within JPSE, plans, coordinates, and synchronizes PA activities with informational power activities to maximize support to campaign objectives and ensure execution of PA roles, responsibilities, and fundamentals. JPSE-PA provides ready, rapidly deployable, expeditionary joint PA capability to CCDRs to support joint operations, facilitate the rapid establishment of joint force headquarters, and bridge joint requirements supporting worldwide operations. JPSE-PA personnel assist development, planning, assessment, and synchronization of operational and mission narratives, themes, messages, PA, and VI activities with the national narrative.

(3) **Joint Warfare Analysis Center.** The Joint Warfare Analysis Center provides CCMDs, the JS, and other customers with effects-based analysis and precision targeting options for selected networks and nodes to carry out the national security and military strategies of the United States during peace, crisis, and war. The Joint Warfare Analysis Center provides timely and accurate engineering and scientific analysis to military commanders and government officials to advance the NSS.

(4) **Joint Electromagnetic Warfare Center (JEWEC).** JEWEC integrates joint effects in the electromagnetic spectrum (EMS) by providing adaptive operational solutions and advocating for the coherent evolution of capabilities and processes to control the EMS during military operations. The JEWEC assesses EW requirements, technology, and capabilities, while conducting modeling, analysis, and EMS activity coordination between CCMDs and other USG departments and agencies. The JEWEC also deploys EW experts, trains staffs, stands up forward planning cells, and delivers rapid warfighter support when required. JEWEC personnel provide CCMDs with options to gain and maintain joint EW freedom of maneuver in the EMS, which is critical to conducting all operations.

(5) **Joint Intelligence Support Element (JISE)/Joint Intelligence Operations Center (JIOC).** The JISE provides the JTF with tailored intelligence products and services with a continuous analytical capability. Capabilities of the element may include order of battle analysis, collection management, target intelligence, OIE analysis, a warning intelligence watch, and a request for information (RFI) desk. Alternatively, in a particularly large or protracted campaign, the JTF commander may decide to employ an operational-level JIOC. An operational-level JIOC incorporates the capabilities inherent in a JISE but is generally more robust. The JISE can provide population-centric, socio-cultural intelligence and physical network lay downs, including the information transmitted via those networks. The JISE/JIOC can greatly facilitate an understanding of the interrelationship between the physical, informational, and human aspects of the environment and assist information planners in determining the desired effects that lead to mission success.

For more information on JISE/JIOC, refer to JP 2-0, Joint Intelligence.

(6) **Defense Media Activity (DMA).** DMA is a mass media and training and education organization that creates and distributes DOD content across a variety of media platforms to audiences around the world.

h. The Joint Force

(1) **JFC.** The JFC establishes and communicates command-specific guidance to ensure all joint force operations and activities are planned and executed to account for the effective management and application of information. This will include assigning responsibility for the tasks related to the information joint function. This may include standardizing organizational practices, establishing routine working groups, or establishing a center with responsibility for the information joint function tasks. Each of the directorates has responsibility related to information joint function tasks, but the JFC should assign overall responsibility and authority to a staff lead to ensure unity of effort. The JFC may choose to create additional staff or functional organizations to conduct or coordinate joint force activities related to the leveraging of information, coordinate with other organizations to obtain support, or synchronize activities with other organizations. This includes creating groups of specialized forces to conduct OIE. The JFC may choose to retain control of any newly created formation under the operations directorate of a joint staff (J-3) or create a separate task force. From this point forward, “OIE unit” will be used to represent a

formation that conducts OIE. The JFC also identifies requirements for information planners to serve as OIE and capability SMEs and planners on the joint force staff or other headquarters staffs. During operational design and joint planning, the JFC provides planning guidance that describes the desired conditions that must exist in the IE to support mission accomplishment, how the joint force will leverage the inherent informational aspects of its activities to support the JFC's objectives, how information activities will support the scheme of maneuver, and the types and level risk that the JFC will accept in the IE. The JFC will also assign missions to OIE units.

(2) **JFC's Staff.** The JFC's staff performs duties and handles special matters over which the JFC wishes to exercise close, personal control. JFCs and their staffs evaluate communication considerations with the interagency partners when planning joint operations. The staff advises the JFC on the inherent informational aspects of their activities, including how words and images will impact the JFC's operational areas. The staff also advises the JFC when their activities may have effects on the IE that impact other AORs. The chief of staff (COS) manages the staff. The staff group may include, but is not limited to, the PAO, staff judge advocate (SJA), KM officer, and POLAD.

(a) **COS.** The COS is the key staff integrator and synchronizer. The COS establishes a framework of trust, shared understanding, and intent within the staff. This is accomplished through the establishment and management of staff processes and procedures, understanding and management of staff capacity, setting priorities, and KM and IM. The COS coaches, mentors, and leads the staff. The COS is also normally empowered to make certain decisions to retain agility in decision making, such as in the areas of targeting and messaging.

(b) **POLAD.** POLADs are senior DOS officers (often flag-rank equivalent) detailed as personal advisors to senior US military leaders and commanders, and they provide policy analysis and insight regarding the diplomatic and political aspects of the commanders' duties. Due to their status and contacts, they can enable interorganizational cooperation relationships and foster unity of effort. The POLAD provides USG foreign policy perspectives and diplomatic considerations and establishes links to US embassies in the AOR or joint operations area (JOA) and with DOS. They articulate DOS objectives relevant to the CCMD's theater strategy or JTF commander's plans.

(c) **PAO.** The PAO is the commander's principal spokesperson, senior PA adviser, and a member of the CDR's personal staff. In that role, the PAO provides counsel to leaders, leads PA and communication activities, collaborates with other information planners to develop the narrative, supports the commander's intent, and supports community engagement and KLE. The PAO may also co-chair the JFC's information CFT. The PAO, in conjunction with others on the staff, quickly and accurately assesses the IE to provide guidance and COAs to the commander. Such assessments enable the commander to better inform relevant audiences about ongoing operations and engender their support. The PAO has the knowledge, skills, resources, and authority to provide timely, truthful, and accurate information, VI, and context to the commander, the staff, and subordinate and supporting commanders. PAOs are able to rapidly release information in

accordance with DOD policy and guidance to the news media and the public. PAOs and PA staffs work with other information professionals to coordinate and deconflict communication activities.

(d) **Joint Force SJA.** The joint force SJA, also titled the command judge advocate, is the principal legal advisor to the CCDR, with a focus on joint operational law issues pertaining to their commander's AOR. In most cases, the joint force SJA is also the principal legal advisor to the deputy commander, COS, and any Service element. The SJA provides advice on laws and policies related to operating in and through the IE, potential legal limitations on information activities, and bilateral agreements that may impact the management and application of information.

For more information on the SJA section, refer to JP 3-84, Legal Support.

(3) **Joint Force Staff Directorates.** Each staff section collaborates routinely, but to varying degrees, to plan, synchronize, support, and assess activities that leverage information.

(a) **Manpower and Personnel Directorate of a Joint Staff (J-1).** The J-1 is the principal staff officer for personnel functions and processes requirements for individual, team, and unit augmentation or attachment. The J-1 builds manning documents and provides advice regarding information forces and support available to the joint force. In coordination with the J-3, the J-1 determines information force and personnel requirements, to include number of personnel, Service, grade, skill, clearance, and any special requirements for each billet description.

(b) **J-2.** The J-2 is the principal staff officer for all matters concerning military intelligence, security operations, and military intelligence training. The J-2 produces the intelligence used by information forces and working groups, and provides intelligence briefings or updates and answers information requirements. It also coordinates with counterintelligence; law enforcement; and information system developers, providers, administrators, and users to ensure timely sharing of relevant information. J-2 supports leveraging information by:

1. Preparing a JIPOE product and a threat assessment of enemy C2 systems that addresses the political, economic, social, and cultural influences, along with the targets and methods for offensive operations. The threat assessment describes enemy decision-making processes with biographical backgrounds of key threat leaders, decision makers, and communicators and their advisors. It should also include a comprehensive comparison of enemy offensive information capabilities against friendly vulnerabilities.

2. Collecting data to establish an EW database, target list, and coordinate intelligence gain/loss assessments for C2 targets.

3. Providing intelligence support to MILDEC operations, specifically helping the communications system directorate of a joint staff (J-6) plan use of friendly

information systems as deception means, and establishing counterintelligence measures to protect the MILDEC operation from detection.

(c) **J-3.** The J-3 assists the commander in the direction and control of operations, beginning with planning and through completion of specific operations. In this capacity, the J-3 plans, coordinates, and integrates operations. As the staff principal charged with ensuring the joint force leverages information during the conduct of all operations, the J-3 responsibilities include, but are not limited to:

1. Ensuring the leveraging of information is addressed as an element along with movement and fires in the joint force scheme of maneuver.

2. Planning all operations to leverage the inherent informational aspects of military activities, and tasking units and assets as necessary.

3. Integrating OIE into joint force plans and assigning missions to OIE units in plans and orders.

4. Coordinating information forces and determining personnel requirements for the joint force. This includes providing appropriate billet descriptions and justifications to the J-1 for sourcing and prioritizing augmentation requests or RFFs.

5. Validating or approving, as necessary, inputs and products from the information planning cell and the JFC's information CFT (these are discussed in paragraphs 3.h.(4) "Information Planning Cell" and 3.h.(5) "Information CFT," respectively) for inclusion into plans and orders.

6. Ensuring effective coordination and synchronization of activities among information planners and other staff sections and CFTs.

7. Overseeing the staff functions of the information planners and the functioning of the information planning cell.

8. OPSEC and the protection of critical/sensitive information.

(d) **Logistics Directorate of a Joint Staff (J-4).** The J-4 develops logistic plans and services, to include the coordination and supervision of supply, maintenance operations, deployment and distribution, engineering, health services, operational contract support, food service, and other operationally required logistic support activities. The inherent informational impacts of these highly visible activities could support or undermine the JFC's objectives. Those informational aspects will encompass political, social, cultural, legal, or other concerns. Consequently, the J-4 should plan sustainment activities to best leverage those aspects to support the JFC's objectives and to protect the joint force from vulnerabilities in and through the IE. J-4 responsibilities with respect to leveraging information include, but are not limited to:

1. Identifying the inherent informational aspects of logistics activities that will potentially affect relevant actor behavior and including those informational aspects in the sustainment annex and in the information estimate.

2. Formulating logistics policies and planning sustainment activities to reinforce the positive and avoid or mitigate the negative impacts of those activities. For example, awarding contracts to support operational requirements to local vendors through an open and transparent contracting process that a local populace trusts would reinforce support for joint force activities, whereas operating a logistics hub in an area or manner that disrupts local agriculture or commerce will undermine support for joint force activities.

3. Advising the information CFT on how military operations will affect logistics efforts and how those logistics efforts can be conducted in a way to support the OIE (e.g., conducting logistics activities in a way that prevents disclosure of joint force intentions).

4. Coordinating with OPSEC planners, as necessary, to identify critical information and indicators to protect essential secrecy.

5. Identifying relevant actors who may be positively or negatively impacted by logistics activities. That includes understanding how relevant actors will perceive those activities.

(e) **Plans Directorate of a Joint Staff (J-5).** The J-5 assists the commander in planning and preparing joint plans, orders, and associated estimates of the situation. The J-5 may also contain an analytic cell that conducts simulations and analyses to assist the commander in plans preparation activities or such a cell may be established as a special staff. J-5 responsibilities related to the leveraging of information include, but are not limited to:

1. Including the inherent informational aspects of joint force activities in estimates of the situation.

2. Planning operations so the leveraging of information is addressed as an element along with movement and fires in the scheme of maneuver.

3. Planning operations to leverage the inherent informational aspects of military activities, and tasking units and assets as necessary.

4. Integrating OIE into the planning of operations and including tasks for OIE units in plans and orders.

5. Assessing the impact in and through the IE of operations, activities, and actions, and determining whether operations, actions, and activities contributed to or detracted from the successes.

6. Participating in the narrative development process to ensure alignment of planning with national/interagency communication guidance.

(f) **J-6.** The J-6 is the principal staff assistant to the JFC for all matters concerning DODIN operations, applicable portions of DCO, network transport, information services, and spectrum management operations within the operational area. As such, the J-6 is a key enabler for the development of a secure, collaborative environment that enhances the JFC and staff situational awareness and ability to leverage information. The J-6 responsibilities relative to the leveraging of information include, but are not limited to:

1. Directing the actions of subordinate DODIN operations and IM staff elements.

2. Coordinating DODIN operations and IM support of information collection with the J-2.

3. When notified, coordinating with the cybersecurity service provider for network intrusion devices, information, approved systems, and software.

4. Identifying the inherent informational aspects of communication activities that will potentially affect the drivers of relevant actor behavior and including those informational aspects in the communications annex and in the information estimate.

5. Advising the information CFT on how the joint communication system can be employed during operations to support the leveraging of information. This includes using the communications system to enable the planning and conduct of information activities and how signature management can be employed.

6. Planning and directing the actions of subordinate DODIN operations and IM staff elements in support of information activities and OIE.

7. Coordinating with other commands to avoid conflicting information and ensure unity of effort.

(4) **Information Planning Cell.** JFCs may establish an information planning cell to provide command-level oversight and collaborate with all staff directorates and supporting organizations on informational considerations during planning and the conduct of operations. The information planning cell, composed of information professionals on the staff, serves as the focal point for planning how the joint force will leverage the inherent informational aspects of its activities and for planning OIE.

(a) The information planning cell is a standing organization subordinate to the operations branch within the J-3 to provide command-level oversight on all aspects of leveraging information.

(b) The information planning cell comprises personnel with subject matter expertise in OIE, specialized capabilities (e.g., CA, MISO, PA, EW, COMCAM, CO), and information activities (e.g., KLE, OPSEC) who serve as staff information planners. The J-3 should tailor the composition of the cell as necessary to accomplish the mission. In cases where specialized capabilities have their own staff entities, SMEs may be assigned to the information planning cell as planners and serve as liaisons to their respective staff section (e.g., a PA planner assigned to the information planning cell would liaise with the PAO and PA staff; an EW planner assigned to the information planning cell would liaise with the JEMSO or joint electromagnetic spectrum operations cell [JEMSOC]).

(c) The information planning cell members collaborate with all staff directorates and supporting organizations to ensure the joint force effectively leverages information as an element of maneuver in support of the JFC's objectives. Information planners provide subject matter expertise throughout operational design and the joint planning process (JPP) (see Chapter IV, "Operational Design and Planning"). The information planning cell supports the J-3 in the direction and control of operations to ensure the impacts, in and through the IE, of all activities support the JFC's objectives and enduring outcomes. Information planning cell members participate in staff joint planning groups (JPGs) or equivalent organizations and may be subtasked to serve as information planners in the JS J-5. The information planning cell chief heads the information CFT and may co-chair the information CFT with PAO. Information planning cell members comprise the core of the information CFT (see paragraph [5], "Information CFT") and is responsible for incorporating input from the information CFT into plans and overseeing execution of information activities.

(d) The information planning cell collaborates with other staff sections to identify the inherent informational aspects of activities that should be included in those staff estimates. Additionally, they identify and maintain the information estimate.

(e) The organizational relationships between the information planning cell and the information forces, to include OIE units, are per commander guidance. Information forces provide input on the employment of their respective capabilities and activities. The information planning cell chief and commander or senior representative of each of the information forces exercises their specific supporting duties and responsibilities.

(5) **Information CFT.** The information CFT is the JFC's forum for the development of a shared understanding of the IE and for the organization, coordination, and synchronization of joint force activities in and through the IE. The information CFT maintains situational awareness of the impact in and through the IE of operations, activities, and investments. As necessary, the information CFT develops and recommends alternatives or follow-on activities that support achieving the JFC's objectives.

(a) The information CFT is comprised of members of the information planning cell and representatives from across the staff directorates, subordinate OIE units and information forces, and USG and other mission partners.

(b) Members of the information CFT should establish ongoing communications with similar forums at the JS and other joint force, interagency, and multinational partners to ensure the joint force remains aware of the actions of others that may have impacts on those factors that make up the IE that will affect the JFC's OE. This awareness also helps identify threats, vulnerabilities, and opportunities in the IE.

(6) **Media Operations Center.** A JFC may establish a media operations center to serve as the focal point for the interface between the military and the media during the conduct of military operations. The media operations center serves as a central meeting place for military personnel and media representatives and provides the media with a primary information source, a logistics support base, transmission capability, and a coordination base.

(7) **JEMSOC.** The JEMSOC synchronizes and integrates the planning and operational use of electromagnetic support sensors, forces, and processes within a specific JOA to reduce uncertainties concerning the threat, environment, time, and terrain. The JEMSOC consolidates, prioritizes, integrates, and synchronizes the component electromagnetic spectrum operations (EMSO) plans and attendant EMS-use requests to produce a consolidated JEMSO plan. Joint force unity of effort in the EMS derives from the JEMSOC's integration of all joint force EMS actions across both the joint force's functional staff elements (e.g., signals intelligence, EMS management, EW, CO, fires) and the joint force's components.

(8) **KLE Cell.** A KLE cell may be established to map, track, and distribute information about the key leaders within the JOA. The KLE cell should establish and maintain a human information database, recommend KLE responsibility assignment, deconflict KLE activities, conduct pattern analysis, develop a detailed background briefing on each key leader, suggest specific approaches for encouraging support for activities and objectives, ensure debriefs are conducted following engagements, and update the map with current information and intelligence and debrief information. The cell provides an updated map (with human information of the area), background information, and desired effects for KLE in the JOA to field units and staffs. The KLE cell coordinates subordinate command KLE activities to ensure a coherent effort across the JOA, gathering of debriefing information, and updating of the data base.

(9) **Counter Threat Finance (CTF) Cell.** CTF cells are a central point to integrate threat finance intelligence into CTF operations and coordinate execution of CTF activities. The principal mission of a CTF cell is to identify and disrupt funding flows, financiers, and financial networks of terrorists, insurgents, and other relevant actors. CTF actions, activities, and operations are designed to deny, disrupt, destroy, or defeat the generation, storage, movement, and/or use of assets to fund activities that support an adversary's ability to negatively affect US interests. When establishing CTF cells, it is important to ensure the relevant participants have been included as a part of the collaborative effort. The CTF cell's staffing structure, toolset, and command hierarchy are designed to leverage tools and resources from across the intelligence, policy, military, and law enforcement communities to complement and enhance the military and other

objectives of the USG. When optimally configured and supported, a CTF cell is a force multiplier that can increase insight into the threat's capabilities, exploitable weaknesses, and intentions. The involvement of various interagency stakeholders enables the CTF cell to leverage multiple authorities and unique capabilities. CTF activities are inherently information activities that can affect the behavior of relevant actors. CTF cell members should be standing members on the information CFT and will advise that forum on how the CTF activities can impact relevant actors. For example, CTF actions that disrupt the flow of illegal funds from malign actors to corrupt government officials may dissuade other government officials from participating in corrupt activities. Or, when CTF actions result in the successful prosecution and conviction of government officials for corruption, a local populace trust in government institutions is increased, resulting in those locals actively supporting and participating in those institutions.

(10) **Joint IM Cell.** Depending on the size of the joint force and scope of operations, the COS may establish a joint IM cell within the joint operations center. The joint IM cell reports to the COS or joint operations center chief (or the J-3) and facilitates information flow throughout the JOA. The joint IM cell ensures the commander's dissemination policy is implemented as intended; takes guidance published in the commander's dissemination policy and combines it with the latest operational and intelligence information obtained from the joint operations center or joint analysis center; works closely with the joint network operations control center to coordinate potential changes in communications infrastructure to satisfy changes in the commander's information dissemination requirements; and coordinates the accurate posting of all current, approved commander's critical information requirements (CCIRs).

4. Service Organizations

The Services man, train, and equip organizations to provide the joint force with the ability to leverage information during joint operations and to conduct OIE. Those Service organizations provide distinct specialized capabilities to the joint force (e.g., MISO, CMO, CO, PA, EW, COMCAM) or provide information commands composed of multiple specialized capabilities that focus on leveraging information and enable the joint force to create effects in the IE. Those Service-provided organizations that are trained and equipped to conduct OIE, as described in Chapter VII, "Operations in the Information Environment," are referred to as OIE units. A United States Marine Corps' (USMC's) Marine expeditionary force information group (MIG) is an example of one such force. For a discussion of the types of Service organizations that provide distinct specialized capabilities, see paragraph 5, "Information Forces," and Chapter VII, "Operations in the Information Environment."

a. United States Army

(1) **Army Cyber Command (ARCYBER).** ARCYBER, the United States Army Service component command assigned to USCYBERCOM, directs and conducts integrated EW, information activities, and CO as authorized, or directed, to ensure freedom of action in and through cyberspace and the IE and to deny the same to adversaries.

ARCYBER defends military networks, secures Army weapons platforms, and protects critical US infrastructure. Army cyberspace forces are deployed globally, conducting DCO and OCO.

(2) **1st IOC [1st Information Operations Command] (Land)** is under operational control (OPCON) of ARCYBER and provides the Army and the joint force with information activities support through deployable teams, reachback planning and analysis, and specialized training. Deployable teams include field support teams with information activities subject matter expertise and vulnerability assessment teams that assist units in identifying and resolving vulnerabilities to improve the command's defensive posture.

(3) **United States Army Special Operations Command (USASOC)**. USASOC oversees the special operations forces of the United States Army and is the Army Service component command of United States Special Operations Command. In addition to Army Special Forces, a military intelligence battalion, and other support troops, USASOC encompasses the 4th and 8th Psychological Operations Groups (Airborne) and the 95th Civil Affairs Brigade (Airborne). The 4th and 8th Psychological Operations Groups (Airborne) provide psychological operations forces and MISO capabilities to CCMDs, US embassies, and other USG departments and agencies to synchronize plans and execute MISO across the competition continuum. The 95th Civil Affairs Brigade enables military commanders and US ambassadors to improve relationships with various stakeholders in local areas to meet the objectives of the USG. 95th Civil Affairs Brigade (Airborne) teams work with DOS country teams, government, and NGOs at all levels and with local populations in permissive, uncertain, and hostile environments.

(4) **United States Army Civil Affairs and Psychological Operations Command (USACAPOC)**. All United States Army Reserve Component psychological operations and CA units are assigned to USACAPOC. The two assigned psychological operations groups (2nd and 7th) and four CA commands (350th, 351st, 352nd, and 353rd) comprise over 80 percent of the total Army CA and psychological operations forces available to DOD, providing the capability to support Army conventional forces across the competition continuum. In addition, the United States Army Reserve's only theater information operations group (TIOG) is assigned to USACAPOC. The 151st TIOG supports several CCMDs with modular and tailorable information planning capabilities in support of Army and joint requirements.

(5) **The United States Army National Guard TIOG**. The Army National Guard contains two TIOGs (56th and 71st). Each TIOG consists of two battalions and deploys mission-focused, modular teams capable of conducting information activities, created from various capabilities resident within the groups. In the field, these teams provide the supported command with information planning, synchronization, assessment, and analysis of the OE.

b. United States Navy

(1) **United States Fleet Cyber Command (US FCC)/United States Tenth Fleet.** US FCC reports directly to the Chief of Naval Operations as a Navy Echelon 2 command and is assigned to USCYBERCOM. US FCC plans, coordinates, integrates, synchronizes, directs, and conducts CO. US FCC is responsible for Navy network operations, OCO and DCO, space operations, and signals intelligence. United States Tenth Fleet is the operational arm of US FCC and executes its mission through a task force structure similar to other warfare commanders. United States Tenth Fleet exercises OPCON of assigned naval forces through its task force structure to create tactical and operational effects in and through cyberspace, space, and the EMS to naval partners and joint forces worldwide.

(2) **United States Naval Information Forces (NAVIFOR).** NAVIFOR mans, trains, and equips information warfare capabilities ashore and afloat. NAVIFOR provides operational commanders ashore and afloat with combat-sustainable forces. The command's areas of expertise include communications, networks and architectures, combat systems interoperability, cryptology/signals intelligence, CO, EW, information-related activities, intelligence, meteorology, oceanography, precise time, astrometry, and space.

WARFARE TERMINOLOGY

Joint doctrine recognizes only two types of warfare – traditional warfare and irregular warfare. Strategic documents and Service publications may use the term 'information warfare' to describe the mobilizing of information to attain a competitive advantage and achieve United States (US) policy goals. In this sense, information warfare encompasses the range of offensive and defensive efforts that use information across the competition continuum to exploit the information environment against adversaries, to inform public opinion, and to compel decision makers to take certain actions. The US military contributes to information warfare by deliberately leveraging the inherent informational aspects of activities and by conducting operations in the information environment.

c. USMC

(1) **Deputy Commandant for Information (DC I).** The DC I develops and supervises plans, policies, and strategy for all OIE-related activities and identifies requirements for OIE doctrine, manpower, training, education, and equipment to support the Marine air-ground task force (MAGTF). In support of the Commandant of the Marine Corps' Title 10, USC, responsibilities as a Service Chief, DC I serves as the principal advisor on all matters and services as the principal spokesperson on Marine Corps OIE-related programs, requirements, and strategy throughout the regarding Marine Corps IE operating programs, requirements, strategies throughout the Department of the Navy and DOD.

(2) **Marine Corps Forces Cyberspace Command (MARFORCYBER).** MARFORCYBER is assigned to USCYBERCOM and conducts the full spectrum of CO,

to include operating and defending the Marine Corps Enterprise Network (MCEN), conducting DCO within the MCEN and joint force networks, and, when directed, conducting OCO in support of joint force and MNF operations, to enable freedom of action and deny the same to adversaries.

(3) **MIGs.** MIGs coordinate, integrate, and employ capabilities to ensure the MAGTF commander's ability to facilitate friendly forces maneuver and deny the enemy freedom of action in the IE. MIGs also provide communications, intelligence, and supporting arms liaison in support of MAGTFs operations. The MIG, in coordination with the MAGTF command element staff, leverages capabilities resident within its subordinate units to conduct offensive, defensive, and exploitative actions within the IE. The MIG, via its subordinate units and the information command center, integrates and employs information capabilities in execution or support of the information joint function. MIG OIE capabilities include communication strategy and operations, which entails PA/VI/COMCAM that provide timely, accurate information, which informs and educates about the missions, organization, capabilities, needs, activities, and performance of the Marine Corps as a part of national defense.

(4) **Marine Corps Information Operations Center (MCIOC).** The MCIOC provides operational support to the Marine Corps forces and MAGTFs and provides OIE subject matter expertise in support of USMC OIE advocates and proponents to enable the effective integration of OIE into Marine Corps operations.

(5) **Civil Affairs Group (CAG).** The CAG provides the MAGTF commander with specially trained and organized CA personnel to facilitate the planning, coordination, execution, and assessment of CA operations. The CAG is a subordinate command of Marine Forces Reserve and functions either as an integral unit or in support of the gaining force commander or will provide separate detachments, separate teams, staff augments, or liaison personnel.

d. **United States Air Force**

(1) **Sixteenth Air Force (16th AF)/Air Force Cyber Command (AFCYBER).** 16th AF is responsible for developing, preparing, generating, employing, and presenting information warfare forces. AFCYBER is assigned to USCYBERCOM to employ cyberspace forces and 16th AF integrates multisource ISR, CO, EW, and information warfare capabilities across the competition continuum. A key mission task includes the integration of information warfare, which is accomplished by the application of the principal Air Force capabilities to create desired effects on the IE.

(2) **616th OC [616th Operations Center]** handles daily intelligence-gathering and offensive and defensive missions in the air, in cyberspace, and across the EMS.

(3) **16th AF Information Warfare Cell.** The 16th AF Information Warfare Cell, attached to Headquarters, 16th AF, helps in operational planning of information warfare

capabilities and integration at operational and tactical levels required to support United States Air Force and joint operations.

e. United States Space Force (USSF)

(1) **Space Delta 6 CO.** Space Delta 6, as part of Space Operations Command (SPOC), executes CO to protect space operations, networks, and communications. SPOC is the United States Air Force Service component to USSPACECOM.

(2) **Space Delta 8 Satellite Communications and Navigational Warfare.** Space Delta 8, as part of SPOC, provides position, navigation, timing, and satellite communications to US military, multinational partners, interagency partners, and commercial/civilian users.

5. Information Forces

Information forces are those Active Component and Reserve Component forces of the Services specifically organized, trained, and equipped to create effects in the IE. These forces provide expertise and specialized capabilities that leverage information and can be aggregated as components of an OIE unit to conduct OIE. Information forces are available to the joint force through the RFF process.

a. **CA.** CA provides expertise on the civil component of the OE. CA forces analyze and evaluate civil considerations for the commander and staff during mission analysis. CA forces promote the legitimacy of the mission by advising commanders on how to best meet their moral and legal obligations to the people affected by military operations. CA conducts civil reconnaissance and network engagement to help define the OE for the commander, to create options to influence the networks in support of US and joint forces information activities. CA coordinate, integrate, and synchronize plans and operations with the civil component. CA produce area studies, area assessments, and analysis that can help identify and describe civil considerations within the OE and refine the IE.

For additional guidance on CA and CMO, refer to JP 3-57, Civil-Military Operations.

b. **Psychological Operations Forces.** Psychological operations forces are trained and equipped to conduct MISO. Their primary task is to influence. They create effects in the IE, bringing significant human factors analysis, assessment, and capability to formulate MISO plans and programs that enhance the development and effectiveness of JFC's missions. MISO planners evaluate the psychological effects of military actions and advise the JFC and staff to maximize influence task effectiveness and minimize adverse impact and unintended consequences. The employment of psychological operations forces is governed by explicit policy and legal authorities that direct and determine how their capability is utilized. Synchronization of MISO with other actions precludes DOD messages or actions, and other agencies' messages and actions from contradicting or weakening each other.

For additional guidance on psychological operations forces and MISO, refer to JP 3-13.2, Military Information Support Operations.

c. **PA.** PA staffs are involved in planning, decision making, training, equipping, and executing operations, as well as integrating PA and communication activities into all levels of command and ensuring narrative alignment. PAOs and PA staffs also work with other planners to coordinate and deconflict communication activities. PA activities are divided into public information, command information, and community engagement activities, supported by research, planning, execution, and assessment to support the commander's intent and concept of operations (CONOPS). PAOs at all levels participate in planning, provide counsel to leaders and key staff members on the possible outcomes of military activities, lead development of the mission narrative, and identify the potential impact on domestic and international perceptions.

For more information on PA, refer to JP 3-61, Public Affairs.

d. **Cyberspace Forces.** Cyberspace forces comprise those personnel whose primary duty assignment is DODIN operations, DCO, or OCO. Cyberspace forces include the units of the Cyber Mission Force (CMF), as well as Service-retained units and various units assigned to CCMDs. CMF units operate under the tactical control of the supported CCDR or in direct support or general support, depending upon the circumstances. Although it is possible for CO, including cyberspace-enabled OIE, to produce stand-alone tactical, operational, or strategic effects and thereby achieve objectives, commanders integrate most CO with other operations to create coordinated and synchronized effects required to support mission accomplishment. Cyberspace operations-integrated planning elements (CO-IPEs) integrate within CCDRs' CO support staff to provide CO expertise and reachback capability to USCYBERCOM. The CO-IPEs are organized from USCYBERCOM, JFHQ-DODIN, and joint force headquarter-cyberspace personnel and are co-located at the supported CCMD.

For more information on CO, refer to JP 3-12, Joint Cyberspace Operations.

e. **EMSO Forces.** JEMSO actions to exploit, attack, protect, and manage the electromagnetic environment rely on personnel and systems from EW, EMS management, intelligence, space, and cyberspace mission areas. EMSO personnel prioritize, integrate, synchronize, and deconflict all joint force operations in the electromagnetic environment, enhancing unity of effort. The result is a fully integrated scheme of maneuver in the electromagnetic environment to achieve EMS superiority and objectives.

For additional guidance on EMSO, refer to JP 3-85, Joint Electromagnetic Spectrum Operations.

f. **COMCAM Forces.** Imagery is one of the most powerful tools available for informing internal and domestic audiences and for influencing foreign audiences. COMCAM forces provide imagery support in the form of a directed imagery capability to the JFC across the competition continuum. COMCAM imagery supports capabilities that

use imagery for their products and efforts, including MISO, MILDEC, PA, and CMO. COMCAM also provides documentation for sensitive site exploitation, legal and evidentiary requirements, battle damage assessment (BDA), operational assessment, and historical records.

For additional information on COMCAM, refer to CJCSI 3205.01, Joint Combat Camera (COMCAM).

g. Space Forces. Space operations and activities that leverage information are mutually reinforcing. Space supports the flow of information and decision making. It may also serve as an activity essential to the delivery of specific information in the IE. Conversely, activities that leverage information to generate effects support achievement of space superiority. USSF Guardians on Service, CCMD, and other staffs ensure commanders and their staffs have a common understanding of space operations and how they should be integrated with other military operations to achieve unity of effort and meet US national security objectives. The Joint Combined Space Operations Center, on behalf of the Combined Forces Space Component Command, coordinates, plans, integrates, synchronizes, executes, and assesses space operations and facilitates unified action for joint space operations.

For more information, see JP 3-14, Joint Space Operations.

6. Interorganizational Collaboration

Interorganizational collaboration seeks to find common goals, objectives, and/or principles between diverse organizations to achieve unity of effort and, through planning and leveraging of cross-organizational capabilities, set the conditions to achieve unified action during execution. The relationship that the joint force establishes with relevant organizations helps it develop a more comprehensive awareness of the OE and understanding of the impact of information on the OE. Ultimately, these relationships help the joint force and the other organizations appreciate the impact of their activities and operations toward achieving shared objectives. This interdependency between the CCMD and other USG departments and agencies to achieve common objectives is a vital element of a whole-of-government effort. From an information planning perspective, unified action is particularly critical since the inherent informational aspects of activities resonate through the IE and may create desirable or adverse effects in the operational area. IT may also be leveraged to enable complex interorganizational coordination through collaborative virtual networking to facilitate reachback to the required SMEs. The JFCs and staff consider the capabilities and priorities of USG components, NGOs, and other interorganizational partners throughout the joint force's planning and execution of OIE.

a. Coordination and Synchronization. The deliberate coordination and synchronization of interorganizational efforts enables inclusion of the various perspectives, interests, and equities of each stakeholder; enhances friendly credibility and narrative; preserves legitimacy; mitigates the potential for conflicting messages; and improves the overall efficiency and effectiveness of whole-of-government efforts. To facilitate the

working relationships among the stakeholders, the JFC will need to establish coordination and synchronization mechanisms to facilitate planning and execution with mission partners. The JFC establishes working relationships, specific organizational structures, and operational practices with external organizations to align activities and achieve unity of effort consistent with the overarching USG narrative. For example, the collaboration and synchronization of information activities can be accomplished through the establishment of cross-functional organizations (e.g., joint interagency task force [JIATF], JIACG) capable of leveraging information.

For more information, see JP 3-08, Interorganizational Cooperation.

b. USG Organizations. Effective integration of the appropriate USG organizations will enhance the overall success of joint force operations. There are a multitude of organizations inside and outside DOD that are relevant to the joint force's management and application of information. The JFC and staff, when appropriate, coordinate information activities and objectives for OIE with organizations that can impact the joint force's leveraging of information.

(1) At the national level, the NSC, with its policy coordination committees and interagency working groups, advises and assists the President on all aspects of national security policy. OSD and the JS, in consultation with the Services and CCMDs, coordinate interagency support required to support the JFC's plans and orders. From an information joint function perspective, it is essential to coordinate activities that support creating the JFC's desired effects, with careful consideration of the inherent informational aspects of those activities. While a supported CCDR is the focal point for coordination of interagency supporting activities, interagency coordination with supporting commanders is also important. Prior to integrating interagency capabilities into their estimates, plans, and operations, JFCs should only consider those partners that can realistically commit their resources to the JFC's mission.

(2) Any USG department or agency planning or conducting activities within the JOA, is considered a relevant organization. This is also true of private-sector entities and NGOs. JFCs and their staffs should consider how the capabilities of other USG components, NGOs, and members of the private sector (e.g., multinational corporations, academia, operational contract support) can be leveraged to assist in accomplishing their mission and broader national strategic objectives. JFCs should also consider the capabilities and priorities of interagency partners in planning and executing information activities. Such organizations do not necessarily need to have a physical presence in the JOA to have an impact. Joint planners need to account for these impacts.

(3) In the case of international organizations, the JFC should determine the significance of their presence in the JFC's JOA and account for that presence in the JFC's planning and execution efforts.

(4) **Civil-Military Operations Centers (CMOCs).** The CMOC is a mechanism to coordinate CMO and can also provide operational- and tactical-level coordination

between the JFC and other stakeholders. Horizontal and vertical synchronization among multiple CMOCs assists in unity of effort. The CMOC is the meeting place of stakeholders, providing a forum for military and other participating organizations. Sharing information is a key function of the CMOC. CMOCs receive, validate, and coordinate requests for support from NGOs, international organizations, indigenous populations and institutions, the private sector, and regional organizations. They also liaise and coordinate between joint forces and other agencies, departments, and organizations to meet the humanitarian needs of the populace. This level of interaction results in CMO having a significant effect on the perceptions of the local populace and improves understanding of the IE. Since this populace may include potential adversaries, their perceptions are of great interest to the information community. CMO can assist in identifying relevant actors; synchronizing communications media, assets, and messages; and providing news and information to the local population.

For more information on CMOCs, refer to JP 3-57, Civil-Military Operations.

(5) **JIACG.** The JIACG is an interagency staff group composed of USG civilian and military experts tailored to meet a validated CCDR's requirement. The primary role of the JIACG is to enhance interagency coordination. JIACGs facilitate unified action in support of plans, operations, contingencies, and initiatives. Members participate in planning and provide links back to their parent civilian departments and agencies to help synchronize JTF operations with their efforts. A JIACG provides the means to establish collaborative working relationships between civilian and military planners. For example, during joint operations, a JIACG, as the bridge between the CCDR and interagency partners, provides the CCDR and subordinate commanders with an increased capability to coordinate and synchronize the joint force's leveraging of information with other USG departments and agencies. When augmented with other partners, such as international organizations, NGOs, and multinational representatives, the JIACG enhances the capability to conduct interorganizational cooperation.

(6) **JIATF.** A JIATF is a potential source for fused interagency information and intelligence analysis. For example, Joint Interagency Task Force-West is United States Indo-Pacific Command's (USINDOPACOM's) lead for DOD support to law enforcement for counterdrug and drug-related activities in the USINDOPACOM AOR. Its assigned mission is to protect national security interests and promote regional stability by providing US and foreign law enforcement with fused interagency information and intelligence analysis and with counterdrug training and infrastructure development support.

Refer to JP 3-08, Interorganizational Cooperation, for a list of USG and international organizations relevant to the joint force's planning of, requirements for, and support in leveraging information.

7. Multinational Partner Considerations

Collective security is a strategic objective of the United States which, generally, requires effective integration of diverse multinational partners. This integration effort is

often complicated since some of these mission partners have policies, doctrine, procedures, and capabilities that differ from those of the United States. During such operations, joint planning is accomplished within the context of multinational operations. There is no single doctrine for multinational action, and each alliance or coalition develops its own protocols and plans. With regard to information activities and the conduct of OIE, US planning for joint operations accommodates and complements the inherent complexity of multinational partner considerations.

a. It is essential for the MNF commander to resolve potential conflicts as soon as possible by establishing standard lexicon and procedures, as well as appropriate shared understanding of each other's capabilities. It is also an operational imperative for the MNF commander to integrate multinational partners into joint planning as early as possible. Early integration enables the efficient and effective use of MNF capabilities and resources throughout planning and operations.

b. Each nation has classified and unclassified capabilities, products, and resources that are useful to the joint force and to the MNF's information activities. For example, NATO's Strategic Communications Division produces an IE assessment that improves joint force understanding by identifying audiences; benchmarking attitudes, perceptions, and behaviors; and identifying communications processes and systems. To maximize the benefits of multinational information activities, each nation must be willing to share appropriate information to accomplish the assigned mission, while excluding the information that each nation is obliged to protect. To enable shared understanding across the MNF, the activities and the structures, systems, and facilities that support them should be classified at the lowest level possible. Information sharing arrangements in formal alliances, such as United States participation in United Nations' missions, are worked out as part of alliance protocols. Conversely, information sharing arrangements in ad hoc multinational operations during which coalitions are working together on a short-notice mission, should be developed during the establishment of the coalition.

For more information on MNFs, see JP 3-16, Multinational Operations.

c. Planners and operators consider the capabilities, limitations, and authorities of partners related to the management and application of information by the joint force (e.g., a partner nation with established policies, laws, and means for information dissemination across its country). The policies of each partner regarding the use of information might not align with US/DOD policy, so joint planners, even while collaborating with a partner, always comply with US/DOD policy. See paragraph 8, "Legal Considerations," for a similar discussion related to laws of the United States and its multinational partners. From an information joint function perspective, initial requirements for coordinating and synchronizing with and integrating other partners into US planning include:

- (1) Understanding partner agendas, priorities, and objectives.
- (2) Clarifying partner narratives, themes, messages, and activities.

(3) Establishing deconfliction procedures for narratives, themes, and messages of the MNF that may differ from those of the United States/DOD.

(4) Identifying threats to, vulnerabilities of, and opportunities for the MNF.

(5) Developing options to deter or defeat MNF threats and to mitigate MNF vulnerabilities.

(6) Identifying MNF authorities, capabilities, and capacities.

(7) Determining appropriate access of partners to US systems, services, and information, to include unclassified and appropriate levels of classification validated as mission-essential.

Refer to JP 3-16, Multinational Operations, for additional information on multinational partners and operations.

8. Legal Considerations

US military information activities are subject to applicable international laws and treaties, US laws and policies, and DOD regulations and policies. Understanding how various policies and laws interact in practice with respect to the IE is a challenging task. To overcome these challenges, commanders and staff consult with legal advisors throughout the planning process. Planners should maintain awareness of relevant international agreements and consult with legal advisors to identify associated legal obligations/constraints that must be incorporated into plans. The DOS publication *Treaties in Force* (<https://www.state.gov/treaties-in-force/>) outlines international agreements currently binding on the United States but is not intended to be a definitive listing of all such obligations (i.e., classified agreements, implementing arrangements, and other agreements are intentionally omitted).

a. Many activities and operations that leverage information require specific review processes and execution authorities. Presidential executive orders and policy memorandums and DOD directives, instructions, manuals, and policy memorandums establish the authorities and permissions to plan, integrate, approve, and execute information activities. During the initial planning process, planners should coordinate information activities and OIE across the joint force, as well as with USG departments and agencies. In some cases, DOD may not be the lead agency and, therefore, may be subject to additional constraints.

b. Conducting OIE involves complex legal issues such as statutory, policy, and budgetary authorities that require careful review and may require national-level coordination and approval. Moreover, legal interpretations can differ because of the range of legal interests potentially affected and the challenges for laws and policies to keep pace with the complexity of, and rapid changes in, IT. Commanders and their staffs should

involve legal advisors and policy experts early in, and throughout, the planning and execution process. A best practice is to include legal and policy experts in CFTs.

c. DOD components will execute information activities in accordance with DODD 3600.01, *Information Operations (IO)*; DODD 5122.05, *Assistant to the Secretary of Defense for Public Affairs (ATSD[PA])*; US law; and other supporting policy, guidance, and directions.

d. DOD personnel will not intentionally disseminate information to influence US domestic audiences, organizations, or individuals, to include US Service members and their families.

e. DOD components conducting information activities that also qualify as intelligence activities comply with all law and guidance applicable to such activities including, but not limited to, Executive Order 12333, *United States Intelligence Activities* (as amended), and DODM 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities*.

Refer to JP 3-84, Legal Support, for additional guidance on legal support to CCDRs.

CHAPTER IV

OPERATIONAL DESIGN AND PLANNING

“The world has changed, and our approach to warfare must change with it. As traditional organized power structures erode, disorder fills the void. We are moving from successive regional conflicts to a future characterized by continual global competition. This circumstance will reward those who can leverage information for strategic advantage.”

**Lieutenant General Timothy D. Haugh,
Lieutenant Colonel Nicholas J. Hall, and
Major Eugene H. Fan**
*16th Air Force and Convergence for the Information War,
Cyber Defense Review, Summer 2020*

1. Introduction

Fundamentally, US strategies are grounded in the knowledge that we are guided by our values and disciplined by our interests. Commanders and their staffs employ operational art to connect tactical actions to strategic objectives. This chapter examines how the joint force translates strategic guidance operationally focused outcomes and describes how commanders and staffs incorporate the information joint function into the planning of operations. This chapter amplifies JP 5-0, *Joint Planning*, with the emphasis on how the joint force integrates information into operational design and planning.

2. Information Planners and Operational Design and Planning

a. All members of the JFC’s staff are responsible for accomplishing or contributing to tasks of the information joint function, to include understanding how information affects joint force operations, understanding how their respective activities impact and are impacted by the IE, and integrating that understanding into their respective portions of joint plans.

b. Information planners assigned to the staff enhance the JFC staff’s ability to carry out information joint function tasks. Information planners are trained professionals from across specialized capabilities (e.g., MISO, CMO, CO, EMSO, PA). Those planners have subject matter expertise with specialized capabilities, experience working with and in OIE units, and an understanding of the inherent informational aspects of capabilities and activities of other units (e.g., a bomber task force or a carrier strike group executing a show of force, an armored task force conducting a feint). Information planners collaborate with the rest of the staff to develop and plan activities in a manner that most effectively leverages the informational aspects of joint force operations, as well as planning OIE, to support achieving the JFC’s objectives. They ensure the joint force remains aware of interagency activities that may either support or potentially conflict with achieving objectives and, when possible, collaborate with external organizations to coordinate and synchronize information activities that support achieving shared objectives.

c. Information planners comprise the information planning cell and are the core of the information CFT with responsibility for incorporating input from the information CFT into the operational design and planning of joint operations and maintaining the information estimate. Some information planners are assigned to serve in the JS J-5, or as liaisons to external organizations, particularly with OIE units and information forces.

3. Operational Design

a. **Overview.** Operational design is the analytical framework that underpins planning. Operational design supports commanders and planners in understanding the JFC's OE as a complex interactive system. Operational design is interwoven within the planning process (see Figure IV-1) to provide a framework in which to plan. The framework enables planners to address the complexity of a commander's OE, support mission analysis and COA development, and develop a CONOPS with the highest likelihood of success. Operational design is continuous and cyclical in that it is conducted prior to, and during, joint operations. As commanders and staffs apply the operational design methodology to develop their operational approach, they account for how information impacts the OE and the potential inherent informational aspects of their activities. In doing so, joint force planners gain an understanding of relevant actors and consider how information is used by, and affects the behavior of, those actors.

b. Operational Design Methodology Steps

(1) Understand the strategic direction and guidance.

(a) Strategic guidance and direction give commanders perspective on national-level goals. Sources of strategic guidance include the JSCP and *Contingency Planning Guidance*, policies and directives, domestic and international laws, communication synchronization guidance, and higher headquarters' orders or estimates. Commanders and staffs translate strategic guidance into plans and orders, to include desired behaviorally focused effects that support commanders' objectives and enduring strategic outcomes.

(b) National and subordinate mission narratives also help guide the joint force on how to conduct operations in a manner that supports USG enduring goals.

1. National Narrative. When employing the US military instrument of national power, the President or national security staff may provide a narrative that includes national-level communication guidance. More often, the strategic national narrative will have to be derived (understood) from guidance such as the NDS, NSC talking points, and speeches. The national narrative informs the development of mission narratives in accordance with the narrative hierarchy shown in Figure IV-2.

2. Strategic Mission Narrative. The DOD, either the JS or OSD, then develops a strategic mission narrative that explains the use of the military and puts global operations in context. CCDRs also develop a strategic mission narrative based upon the national narrative. This strategic mission narrative and its supporting themes are included

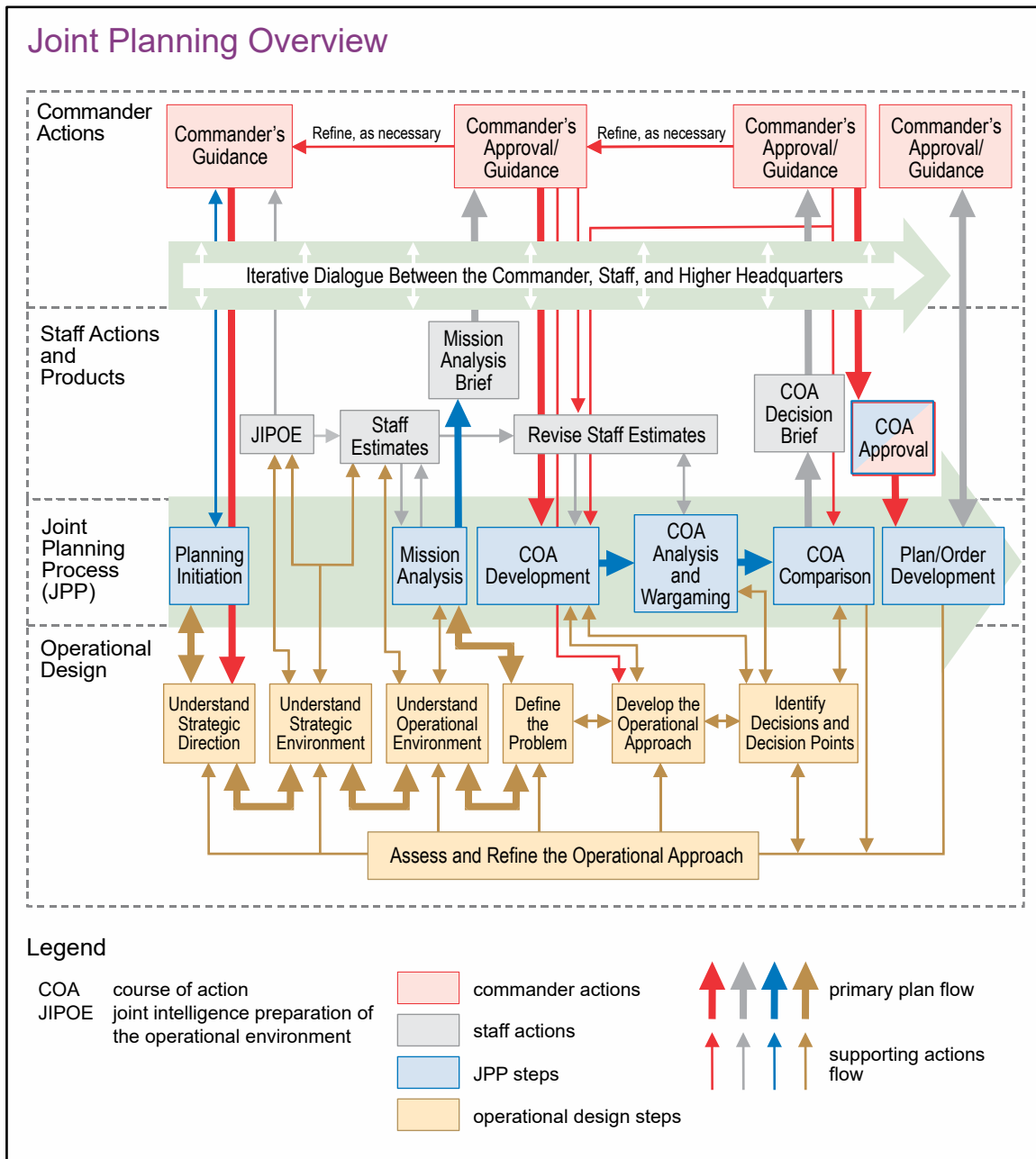


Figure IV-1. Joint Planning Overview

or referenced in the military orders or other strategic direction to lend continuity to campaigns and communications.

3. Operational and Tactical Mission Narratives. CCMD and operational-level headquarters staffs develop cascading operational-level mission narratives with associated themes and messages that nest under the strategic military narrative. As necessary, each tactically focused unit develops and incorporates a local mission narrative that nests under the operational mission narrative.

Narrative Hierarchy		
Narrative Type	Primary Audiences	Sources
National	Global Domestic	President National Security Council
Strategic Mission	Global Theater Domestic	Secretary of Defense Chairman of the Joint Chiefs of Staff Combatant Commanders
Operational Mission	Theater Regional Domestic	Combatant Commands Joint Force Commanders Component Commanders
Tactical Mission	Local Area	Joint Force Commanders

Figure IV-2. Narrative Hierarchy

For more information on narratives, see Appendix A, “Narrative Development.”

(2) **Understand the strategic environment.** The strategic environment is the composite of the conditions, circumstances, and influences that affect national interests beyond the JFC’s OE and may impact the composition of alliances, establish competing requirements or priorities, and/or affect deployment and distribution operations (e.g., degrade or disrupt force flow). The second step in operational design methodology, understand the strategic environment, provides the JFC and staff the strategic context for the assigned mission and provides the boundaries within which the JFC’s operational approach must fit. Information planners work with intelligence analysts to contribute to understanding the strategic environment. These analyses include conclusions on how information is likely to impact the strategic environment and a broad analysis of opponent, friendly, and neutral efforts to influence domestic, regional, and world opinion.

(a) Analysis of the IE is conducted using several analytical processes and models. The result of those analyses provides conclusions about how information in the strategic environment is likely to impact the JFC’s OE and operational approach and how joint force operations are likely to impact the strategic environment. Analysis includes the following considerations:

1. What events or activities (whether related to friendly, neutral, or adversary actors) are resonating in and through the IE that could impact the strategic environment and how those events could affect USG national security objectives, priorities, or the JFC’s operational approach (e.g., a global pandemic, the eruption of a volcano that impacts air travel, national elections in an allied nation, an adversary’s conduct of a ballistic missile or nuclear bomb test).

2. What USG activities, both ongoing and those directed in strategic guidance, will resonate in and through the IE to impact the strategic environment and how they are likely to impact the JFC's OE.

INFORMATION WITH STRATEGIC IMPACT

Russian intelligence agencies and state sanctioned organizations have waged a steady campaign of attacks on information systems around the globe for many years. These have been in retaliation, such as the 2007 targeted attacks and denial of service of the Estonian parliament, banks, ministries, newspapers and broadcasters websites after the Estonian government removed a Soviet-era statue in its capital city; in support of Russian combat actions in neighboring Georgia, Crimea, and eastern Ukraine; to steal information and data as it did when it hacked and inserted malicious code of tech company SolarWinds software in 2020 used by private-sector and United States Government organizations; and to influence domestic politics of other nations, such as its disinformation campaign largely waged on social media leading up to the 2016 United States (US) national elections. More domestic examples are digital breaches of the White House, Department of State, and Joint Chiefs of Staff in 2014 and 2015, as well as the hack of the Democratic National Committee e-mail in 2016.

These are steady and synchronized actions with strategic objectives by Russia. First and foremost, Russia wants to return to a world power status. Disinformation is one way to blunt US influence as a world power both in Allied and partner perceptions of the United States, as well as to foment division and turmoil domestically. Second is to protect Russia's sphere of influence. By forcing the United States to focus more on domestic disorder, it creates a vacuum in which Russia can exert pressure on the world order. Russia targets our North Atlantic Treaty Organization partners and the European Union to sow discord and negatively affect Western liberal democratic institutions. Russia uses disinformation and cyberspace operations to target weaker nearby nations to pressure leadership to reject integration with the West. Third, Russia uses information to protect and strengthen its current regime. Vladimir Putin relies on his hand-picked oligarchs to maintain control of the country. By targeting Western democratic nations it seeks to show the current government in Russia is more stable and able to protect its citizens. Finally, information activities strengthen its military capabilities. Russia does not have the economic means to procure and maintain the traditional military capabilities that the West possesses, so disinformation and cyberspace operations are "cheaper" tools to engage in adversarial competition below the level of armed conflict. In many ways, Russia has an advantage in using information capabilities since it does not subscribe to the same norms and values inherent in democracies. The much quoted adage of "a lie can travel halfway around the world while the truth is putting on its shoes," rings true.

Various Sources

(b) Analyzing the ability of an opponent to influence their domestic audiences, as well as their ability to influence regional and world opinion through the conduct of diplomatic, informational, military, or economic activities.

(c) Analyzing the ability of US and partner nations' diplomatic, informational, military, or economic activities to influence regional or world opinion.

(3) **Understand the OE.** A JFC's OE is a diverse, interactive, and constantly evolving collection of systems. It encompasses the immediate operational area and all conditions, circumstances, and influences that impact the employment of forces or have the potential to impact and affect the JFC's decisions. To frame the problem, the JFC requires an understanding of the current state versus the desired state of the OE. It is also important to appreciate the competing conditions competitors, adversaries, and enemies seek to realize through their operations. Before defining the problem and developing an approach to solve it, the commander and staff first need to describe conditions in both the current state of the OE and the desired state of the OE when operations conclude. Those desired conditions should facilitate the desired relevant actor behaviors. Identifying necessary conditions early in planning will help the commander and staff devise an operational approach with lines of effort (LOEs) and lines of operation (LOOs) that link each current condition to objectives. Information planners assist in the analysis of the informational, physical, and human aspects of the environment; identifying and describing relevant actors and their drivers of behavior; and determining the most likely behaviors of relevant actors.

(a) **Characterize the human, informational, and physical aspects of the OE.** The JIPOE process provides the basis for understanding information and how it affects the JFC's OE. Even though the intelligence directorate of a JFC's staff manages the JIPOE process, other directorates and agencies contribute valuable expertise to develop and assess the complexities of the JFC's OE. Information planners use their specific expertise to assist the planning team to:

1. Understand how information moves in and through the OE. Planners should identify how it is received, processed, and employed; by whom or what; and for what purposes.

2. Establish a baseline of the IE to create a reference point of relevant actor perceptions, beliefs, attitudes, and behavior, while assessing changes to the baseline over time.

3. Distinguish what information in the IE is relevant and characterize its sources and methods of movement or transmission.

4. Identify misinformation and disinformation and credible from non-credible sources of information.

5. Understand the information networks and systems that are being used by relevant actors.

6. Identify which joint force activities are observable and by whom. This includes understanding the inherent information aspects of those activities that are most likely to be used by relevant actors to derive meaning.

(b) Identify and understand relevant actors. These efforts include the conduct of all-source intelligence operations and engagement with partners to improve knowledge of friendly, neutral, and adversary actors and their PMESII systems and how they work as networks. Products that can help identify and describe relevant actors are JIPOE products, target systems analysis, center of gravity (COG) analysis, network engagement analysis, TAA, publicly available information, and area studies and assessments. Information planners use their specific expertise to assist the JPG to:

1. Identify humans and automated systems that are potential relevant actors.

2. Describe what drivers of behavior are most likely to affect relevant actors (see Chapter I, “Fundamentals of Information,” Figure I-2, for examples of drivers of behavior).

3. Understand how relevant actors sense and process information to trigger a behavior that can positively or negatively impact joint operations.

4. Describe how relevant actors communicate and make decisions.

5. Identify relevant actors that are decision makers, key influencers, or both.

6. Identify those key influencers of relevant actors both inside and outside the AOR.

(c) Identify range of potential behaviors of relevant actors. Identifying the range of potential behaviors of relevant actors helps planners formulate the operational approach that will result in desired behaviors. Intelligence analysts help the JPG to develop a detailed understanding of the range of behavior relevant actors may display and assess which of those behaviors are most likely or might have the greatest positive or negative impact on joint force objectives. Information planners use their specific expertise to assist the JPG to:

1. Identify the perceptions that relevant actors are likely to form based on the inherent informational aspects of activities and OIE included in the operational approach.

2. Identify what relevant actor behaviors can be anticipated as a result of those perceptions.

3. Describe how the behaviors of relevant actors are expected to evolve over time.

4. Describe how information can affect behavioral trends to yield outcomes favorable or unfavorable to friendly interests.

5. Identify what broad actions the joint force should take to create the effects in the JFC's OE that arrest or encourage behavioral trends.

6. Identify potential second- and third-order effects of the operational approach, inside the JFC's operational area and globally, including domestically.

(4) Define the problem

(a) Defining the problem involves understanding and isolating the root causes of the issue that are the essence of what may be a complex, ill-defined problem and determining how and why the particular problem requires a joint force solution. Defining the problem begins with a review of the tendencies and potential of the relevant actors and identifying the relationships and interactions among their respective strategies, objectives, and desired conditions. This review helps define areas of tension, competition, and contested environments, as well as the opportunities and challenges these present to the joint force, and helps identify the difference between the current conditions and desired conditions. Framing the problem statement in terms of human behavior and conditions of the environment helps the joint force understand the nature of the problem.

(b) The JFC and staff identify and articulate the following when developing the problem statement:

1. Tensions between current conditions and desired conditions at the objective.

2. Elements within the OE that must change or remain the same to achieve the objective, including relevant actors' behaviors, which impede or support changing the current conditions in the OE to the desired conditions in the OE.

3. Opportunities and threats that the joint force can exploit or that will impede the JFC from achieving the required objectives.

4. Operational limitations.

5. Sources of stability and sources of instability within the OE.

(c) Information planners provide the following inputs for the analysis portion of this step:

1. The description of the informational, physical, and human aspects of the environment, and their effects on relevant actor behavior, that were part of the systems perspective in the previous step.

2. The description of the desired conditions expressed in terms of relevant actor behaviors.

(d) Information planners' contributions to the outputs in paragraph (b) include:

1. Description of the linkages between the root cause of the problem and relevant actor behaviors.

2. A description of the differences between current conditions and those desired conditions that need to be reconciled to support achieving the JFC's objectives, to include cultural, religious, or other human aspects that drive relevant actor behavior. This includes a description of the tensions between current and anticipated relevant actor behaviors and the JFC's objectives and desired conditions.

3. A description of what must change in the IE to facilitate achieving the JFC's objectives. Examples include availability of a reliable communications infrastructure to enable free-flowing information, availability of accurate information to counter adversary propaganda, and a credible and compelling narrative that counters the adversary's narrative.

4. A description of the opportunities and threats in and through the IE that would hinder achieving the JFC's objectives. Opportunities might include an adversary's reliance for C2 on a portion of the EMS that the joint force can control or a populace support of the joint force presence to counter enemy forces. Threats could include sophisticated enemy EMSO capabilities against a joint force relying on the EMS for C2 or a local population's acceptance of an insurgent narrative that describes the joint force as foreign invaders. Opportunities or threats could also include narratives in the OE from third parties or neutral groups that do or could potentially reinforce friendly or adversary narratives. Constraints could include directives to the joint force that dictate actions that have affects in and through the IE (e.g., a requirement to conduct OCO to eliminate a threat, the requirement for the joint force to hold weekly PA briefings or embed reporters with operational units) or directives that restrict actions that cause impacts in or through the IE (e.g., prohibition on the use of OCO that targets relevant actors outside of the JFC's operational area, prohibition on establishing radio stations that compete with local national stations for listenership, restrictions on using religious or sensitive cultural topics in psychological operations messages).

(5) **Identify assumptions.** Where there is insufficient information or guidance, the commander and staff identify assumptions to assist in framing solutions. At this stage, assumptions address strategic and operational gaps that enable the commander to develop the operational approach. During this step of operational design methodology, information planners contribute to the development of the operational approach by drafting assumptions focused primarily on the ability of the joint force to leverage information. These include assumptions about the availability of the means to affect relevant actor behavior; the access the joint force will have to the relevant actors through those means; the joint force authorities and permissions to conduct information activities; and the funding, staffing, and time needed to affect relevant actor behavior. Also, though behavior can be changed in the relative near term, attitude change might take generations to become enduring. All assumptions should be carefully assessed for internal biases and mirror imaging. Other assumptions include the joint force ability to manage and protect friendly information, information systems, and information networks and the forces required to conduct those activities.

(6) **Develop the operational approach.** The operational approach is a commander's description of the broad actions the force can take to achieve objectives. This step of operational design develops the initial model for execution of a campaign or operation that a JFC and staff will continually refine and is the basis for beginning, continuing, and completing detailed planning in the JPP.

(a) The JFC's operational approach is the commander's visualization of how the joint force's operations will transform current conditions into desired conditions—the way the commander envisions the OE at the conclusion of operations to support national objectives. When developing the operational approach, planners identify and describe the logic of the effort—the theory of change—by starting with the desired future state of the OE and working backwards to the current state. A theory of change describes how planners think elements of an operation or LOE will lead to a desired future state. The descriptions should explain how actions or inputs to the activity are expected to lead to changes that support desired outcomes, either directly or through a chain of linked events. These expected changes and their linkages inform assessments to identify progress in producing the desired results and provide indicators of challenges or problems. Information planners use their expertise to describe how information activities link to desired relevant actor behaviors that support the JFC's objectives.

(b) Information planners' contributions to developing the operational approach include analysis of the informational, physical, and human aspects of the environment. These products help the JFC determine how to leverage information as part of the operational approach.

1. **Leveraging information as the main effort.** In operations where a relevant actor is the adversary's COG, the JFC may choose an operational approach that leverages information against the relevant actor to drive desired behaviors. In such cases, joint force efforts will focus on deterring or defeating an opponent coercively by leveraging information to isolate, disrupt, degrade, and control behavior. During armed conflict, this

approach may include the application of lethal or nonlethal force against the COG. Carefully applied force can contribute to deterring an actor from taking unwanted actions.

2. Leveraging information as a supporting effort. In other operations, directly leveraging information to affect the opponent COG or critical capability may not be sufficient to produce the behaviors in relevant actors needed to achieve objectives. In these cases, the JFC may describe an operational approach that leverages information in a supporting role during operations, as well as to maintain the support from allies and other mission partners for those operations. During operations not focused on the defeat of an opponent force (e.g., humanitarian assistance, personnel recovery, noncombatant evacuation operation), the JFC's operational approach should leverage information to inform the supported government and population of joint force efforts to facilitate the efficiency and effectiveness of those efforts and to transition the efforts to full civilian control as quickly as possible.

3. Leveraging information LOE. Regardless of how the JFC addresses the joint force leveraging of information in operational design, a commander should always integrate information and its effects into all LOEs. The JFC may even consider using an information LOE in plans. An information LOE focuses efforts on producing relevant actor behaviors by linking strategic- and operational-level objectives, tasks, effects, and conditions to achieve enduring strategic outcomes. In operations involving many nonmilitary factors, an information OE may be the only way to link tasks, effects, conditions, and the operational objectives.

(7) Identify decisions and decision points. During planning, commanders inform leadership of the decisions that will need to be made, when they will have to be made, and the uncertainty and risk accompanying decisions and delay. This provides leaders a decision matrix to provide warning and enable decisions in advance. Additionally, this helps facilitate collaboration with interagency partners and allies to develop alternatives and exploit opportunities short of escalation. The decision matrix also identifies the expected indicators needed in support of operation assessment and intelligence requirements and collection plans.

(a) Information planners provide input on the decisions and decision points related to the joint force leveraging of information. Examples include decisions on the use of OCO techniques that could reveal a previously undisclosed friendly system, tactic, technique, or procedure; whether to degrade an enemy's C2 through the use of EMS capabilities that would reveal the conduct of covert operation; the timing of a PA briefing to announce the initiation of operations; or whether to conduct MISO ahead of major combat operations.

(b) Information planners also consider and recommend decisions and decision points related to protecting the force from the impacts of activities, to include joint force activities, in or through the IE. These would include decisions to increase cyberspace protection condition system levels in response to enemy or adversary actions, decisions on the timing of disclosing joint force crisis action deployments to delay adversary

understanding of friendly movements and force posture in support of force protection, and decisions on procedures for publicizing joint force-caused civilian casualties to mitigate the impact of the incident on joint force credibility and legitimacy.

(c) Information planners need to consider how operations support options for commanders to provide an enemy or adversary an acceptable means to de-escalate.

(8) Refine the operational approach. Throughout the planning processes, commanders and their staffs conduct formal and informal discussions at all levels of the chain of command, supporting CCDRs, and subordinate commands. These discussions help refine assumptions, limitations, and decision points that could affect the operational approach and ensure the plan remains feasible, acceptable, and suitable. Information planners participate in the refinement of the operational approach by updating the information estimate and providing the results of information activities.

(9) Develop planning guidance. Ideally, the commander issues initial planning guidance, either written or oral, prior to the start of the JPP. At a minimum, the commander provides planning guidance at the conclusion of mission analysis. The commander will refine that guidance as understanding of the OE, the problem, and visualization of the operational approach matures. Planning guidance should include a description of the commander's understanding of the strategic and OEs, a definition of the problem, and a description of the operational approach. Information planners help develop the specific content to inform and guide how the joint force will leverage information to achieve objectives. That content should include a description of:

(a) The OE and how informational, physical, and human aspects impact one another and cause tensions.

(b) The problem framed in terms of relevant actor behavior. This should include the tensions between relevant actor behaviors and the JFC's objectives, along with a timeline for resolution.

(c) Behaviorally focused objectives, which specify relevant actor behaviors required to bring about desired conditions.

(d) Decisive points in the IE that provide the joint force with relative advantage in influencing relevant actor behavior (e.g., gaining access to a threat's information system or network that can be exploited to affect decision making, gaining active support from a key figure whom relevant actors support).

(e) LOEs or LOOs that focus the force on leveraging information to affect behavior.

(f) A summary of limitations regarding the conduct of information activities. For example, constraints might include the requirement for a deliberate communication effort to mitigate the occurrence of civilian casualties in the operational area or to exploit the use of weapons systems for their deterrent effect on adversaries or enemies outside of

the operational area. A restraint might include the prohibition on the use of certain social media or the possession of unapproved personal electronic devices by joint force members during an operation. Additionally, the inherent informational aspects of some activities may lead to additional restraints or constraints if the inherent informational aspects of those activities have transregional effects.

(g) A statement of where the commander will and will not accept risk in leveraging information during operations and conducting OIE. For example, a JFC may identify local population support of a HN's government as a key objective. Consequently, the JFC may be willing to accept the risk of an inefficient, HN-led, US-supported disaster relief effort to avoid a greater risk of an efficient US-led effort causing the local populace to perceive their government as incapable of meeting their needs.

(h) The commander's initial intent that includes desired relevant actor behaviors and the narrative statement or paragraph that conveys the commander's reasons and desired outcomes for the campaign/mission/operation.

c. Informational Considerations During COG Analysis. Identification and analysis of friendly and adversary COGs is a key step in operational design and informs the JPP. A COG is a primary source of power that provides moral or physical strength, freedom of action, or will to act. COGs can be a military force, an alliance, political or military leaders, a set of critical capabilities or functions, or national will. Success requires protecting the friendly COG while defeating the enemy COG. The protection of friendly strategic COGs such as public opinion and US national capabilities typically requires efforts and capabilities beyond those of just the supported CCDR.

(1) COG analysis is used to identify potential threat and friendly COGs, identify critical capabilities, identify critical requirements for each critical capability, and identify critical vulnerabilities for each critical requirement. Based upon how the threat organizes, fights, makes decisions, and uses its physical and psychological strengths and weaknesses, planners identify the threat's and joint force's COGs for further analysis. Planners should recognize that relevant actors may be a COG or key factor for an operation and that using information or denying information to deceive, confuse, or disrupt the ability of the relevant actor to sense and make sense of the situation may be a decisive factor in that operation. Planners analyze COGs within a framework of three critical factors—capabilities, requirements, and vulnerabilities.

(2) Information planners do not conduct a separate COG analysis but actively participate in and contribute subject matter expertise to the joint force, J-2-led COG effort. Additionally, information planners use their understanding of relevant actors to reduce the potential for inadvertently injecting internal biases such as mirror imaging.

(a) **Identify Critical Capabilities.** A critical capability is a means that is considered a crucial enabler for a COG to function as such and is essential to the achievement of the specified or assumed objective(s). Information planners identify critical capabilities by analyzing each COG to determine what primary abilities or

functions are possessed by both friendly and threat forces that can prevent the joint force or the threat from understanding how information impacts the JFC's OE, supporting its decision making, or effectively leveraging information. To test the validity of a critical capability, the staff asks, "Is the identified critical capability a primary ability in context with the given missions of the threat or the joint force? Is the identified critical capability directly related to the COG?"

(b) Identify Critical Requirements for each Critical Capability.

Information planners analyze each critical capability to determine what conditions, resources, or means enable the friendly or threat critical capability. To test the validity of a critical requirement, the staff asks, "Will an exploitation of the critical vulnerability disable the associated critical capability? Does the joint force have the resources to affect the identified critical vulnerability?" If either answer is no, then the information planner reviews the threat's identified critical factors for other critical vulnerabilities or reassess how to attack the previously identified critical vulnerabilities with additional resources. Information planners also look at the critical requirements for friendly capabilities to identify what must be protected.

(c) Identify Critical Vulnerabilities for each Critical Requirement.

Planners then analyze each critical requirement to identify its vulnerability to attack. Information planners help identify critical vulnerabilities that will do the most decisive damage to a COG's ability to access, generate, share, and restrict access to information. Additionally, information planners help identify critical vulnerabilities associated with a COG's critical capabilities associated with the ability to leverage information to affect behavior. However, in selecting those critical vulnerabilities, planners also compare their criticality with their accessibility, redundancy, resiliency, and impact on other military and national objectives. If the exploitation of a critical vulnerability would disable the associated critical requirement, information planners determine if the joint force has sufficient resources to leverage information to affect identified vulnerabilities.

4. Joint Planning Process

a. **Overview.** The JPP is an orderly, analytical process that consists of a logical set of steps to analyze a mission, select the best COA, and produce a campaign or joint OPLAN or order. Like operational design, it is a logical process to approach a problem and determine a solution. It is a tool to be used by planners but is not prescriptive. Throughout the JPP steps (see Figure IV-3), information planners assist other joint planners in incorporating their understanding of how information impacts the OE to identify how to best support human and automated system decision making and how to best leverage information to achieve the JFC's objectives during operations. The result of the JPP is a plan or order that clearly specifies how the joint force will use and leverage information as part of the overall operation. There are information considerations for each of the seven steps of the JPP that are covered in the remainder of this chapter.

b. JPP Steps

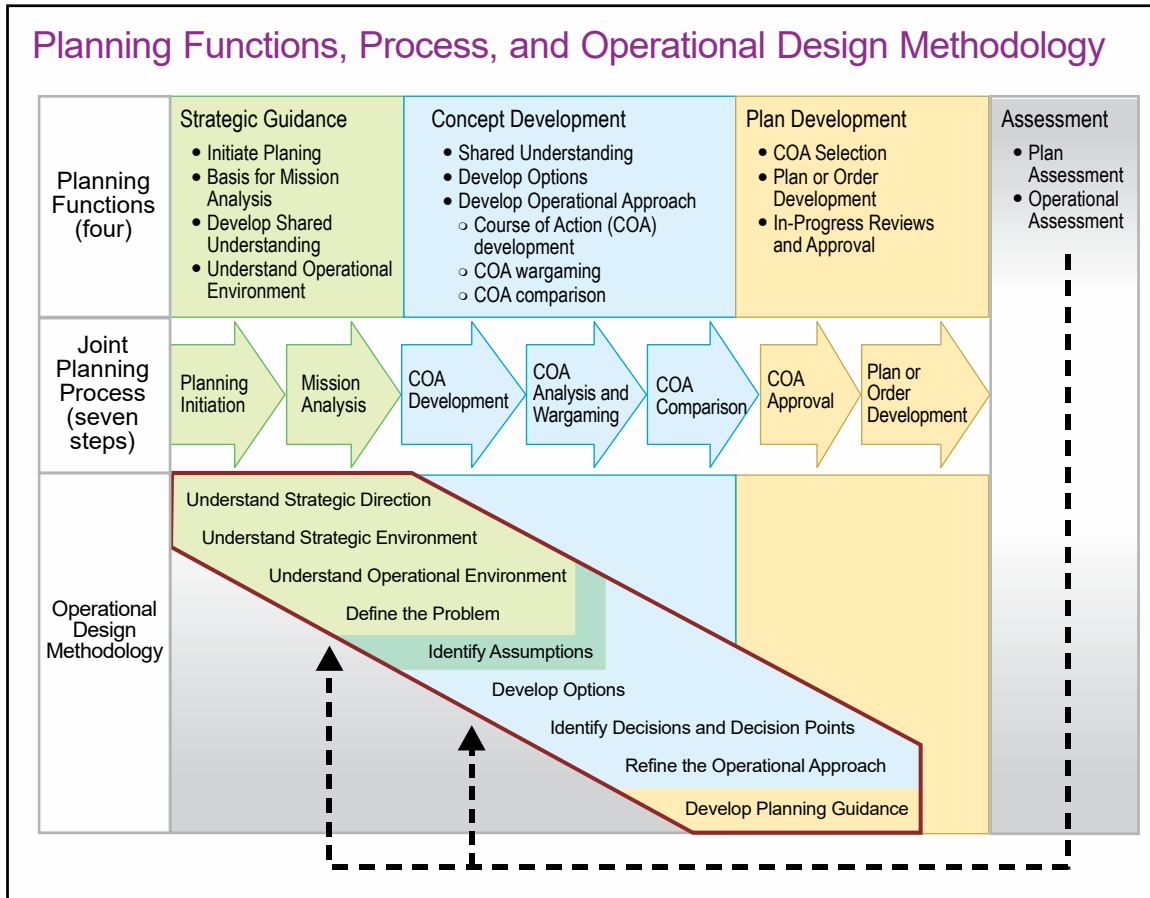


Figure IV-3. Planning Functions, Process, and Operational Design Methodology

(1) **Step 1—Planning Initiation.** During planning initiation, information planners use their specific expertise to assist the JPG in:

(a) Reviewing commander’s planning guidance for information activities and explicit and implied tasks that will impact planning.

(b) Identifying external stakeholders the joint force should collaborate with for planning and executing information activities (e.g., DOS Global Engagement Center, country teams, JIATF or JIACG). See Chapter III, “Unity of Effort,” for organizations to consider.

(c) Determining initial information planning support requirements to augment the staff (e.g., information professionals to serve as information planners, language/regional/cultural expertise).

(d) Gathering and analyzing the information required to plan operations that affect relevant actor behavior and identified networks.

(e) Updating the information estimate, providing updates on changes in the IE, updating the status of information forces, and providing the results of any ongoing information activities.

(2) **Step 2—Mission Analysis.** The JFC and staff develop a restated mission statement that allows subordinate and supporting commanders to begin their own estimates and planning efforts for higher headquarters' concurrence. The joint force's mission is the task or set of tasks, together with the purpose, that clearly indicates the action to be taken and the reason for doing so. Mission analysis is used to study the assigned tasks and to identify all other tasks necessary to accomplish the mission. Mission analysis focuses the commander and the staff on the problem at hand and lays a foundation for effective planning.

(a) Analyze Higher Headquarters' Planning Directives and Strategic Guidance

1. Information planners contribute to the analysis of strategic guidance and higher headquarters' planning directives by understanding and advising the JFC on how national leadership and higher headquarters intend for the military to support the informational instrument of national power. In particular, information planners determine higher headquarters' perspective of how the military will leverage information to achieve national strategic and military objectives, what behaviors that higher leadership wants from relevant actors to support those objectives, and what role the joint force has in leveraging information to obtain those desired behaviors.

2. During this step of mission analysis, CCMD and operational-level headquarters staffs use strategic guidance to begin developing the operational mission narrative. The operational mission narrative will include themes and messages that nest under the strategic mission narrative. The development of the operational mission narrative is a collaborative effort that should include planners with regional and cultural expertise. Operational mission narratives focus on the theater/region and seek to advance the legitimacy of the mission while countering adversary narratives. A compelling narrative at this level guides planning, targeting, and execution. Likewise, the joint force should make every effort to ensure operations, activities, words, and images are perceived as being consistent with the narrative, thereby preventing audiences from perceiving a conflict between the joint force's actions and its words.

a. When developing the operational mission narrative, planners should recognize that narratives are not created in a vacuum. There are pre-existing narratives in the OE and others may emerge. These narratives may be from adversaries, friendly forces, or relevant neutral groups. These other narratives may reinforce or run counter to the joint force narrative. Awareness of these narratives leads to greater understanding of how to leverage operations and messaging activities to achieve friendly objectives.

ALIGNING ACTIONS TO THE NARRATIVE

When General Stanley A. McChrystal assumed command of the International Security Forces Afghanistan (ISAF) in 2009, he recognized that "the side with the most compelling narrative will succeed" and conveyed messages with increased timeliness and transparency while ensuring they matched actions. Preoccupied with force protection, ISAF had operated in a manner that distanced itself, both physically and psychologically, from the people they were seeking to protect. Force protection measures conflicted with General McChrystal's narrative of security and confidence. When ISAF forces traveled through even the most secure areas of Afghanistan firmly ensconced in armored vehicles with body armor and turrets manned, they conveyed a sense of high risk and fear to the population. McChrystal believed that unarmed Afghans would not feel secure if ISAF forces presented an image of insecurity even in relatively secure areas. ISAF needed to be willing to share risk, at least equally, with the local people. Adjusting force protection measures downward to match local conditions sent a message of confidence and normalcy to the population that aligned with the narrative.

Various Sources

b. Analyzing existing narratives provides insight into the messages that relevant actors are conveying, how they are disseminated and propagated, how the intended audiences and relevant actors react to the themes and messages in those narratives, and potential avenues for influence. In addition to informing mission analysis and the development of the operational mission narrative, the results from narrative analysis should be incorporated into JIPOE and operational assessment processes. Figure IV-4 shows some sample questions that an analysis of existing narratives can answer.

3. Additionally, information planners identify operations worldwide in execution and ongoing activities, to include information activities, which will limit the JFC's range of possible COAs, as well as impact plans and operations. This awareness of other ongoing operations and activities includes those of multinational partners.

4. Finally, as part of mission analysis, information planners identify existing authorities and permissions and what additional authorities and permissions that the JFC will require for the conduct of information activities. This is done as early as possible in the JPP because of the time required to obtain those additional authorities and permissions. Use of some capabilities or activities that leverage information to affect behavior may require unique authorities and permissions. Joint force planners should also review the authorities for the use of capabilities and conduct of activities in their own AOR that could affect the OEs of other JFCs through the IE. Achieving a shared understanding of authorities vertically across echelons of command and horizontally across mission partners is key to successful execution. Information planners can advise the planning team on which authorities for leveraging information may require additional time, legal review, or subject matter expertise to request.

Questions for Narrative Analysis

- (a) How do the relevant actors frame and explain their ideology?
- (b) How do relevant actors make their ideology appear enduring and natural to the local culture?
- (c) Do joint force activities challenge their assumptions, beliefs, and meanings?
- (d) What are the local culture/society goals that the joint force can leverage?
- (e) Are there inconsistencies in a relevant actors' narrative? If so, how does the relevant actor deal with those inconsistencies? Do those inconsistencies present a vulnerability that can be exploited?
- (f) What is the structure of the existing narratives?
- (g) How do existing narratives resonate with relevant actors?

Figure IV-4. Questions for Narrative Analysis

(b) **Review Commander's Initial Planning Guidance.** Information planners use the commander's initial planning guidance as the basis for continuing the analysis of the OE begun during operational design, which focused on describing the relationship between the informational, physical, and human aspects of the environment and on identifying and describing relevant actors and their range of potential behaviors (see paragraph 3, "Operational Design").

(c) **Determine Known Facts and Develop Planning Assumptions.** Information planners provide facts and assumptions related to the joint force understanding of how information impacts the OE, the joint force's ability to manage and share information to support decision making, and the joint force's ability to leverage information. Potential facts and assumptions include but are not limited to:

1. The identity of relevant actors and why they are relevant to the JFC's mission.

2. The degree to which the joint force understands the perceptions, attitudes, beliefs, and other drivers of relevant actor behaviors (see Chapter I, "Fundamentals of Information," paragraph 3.d., "Information can affect behavior," for examples of drivers of relevant actor behaviors).

3. The access that the joint force will have to humans and automated systems to affect the behavior of relevant actors.

4. The impact that joint force operations will have upon the OE and relevant actors. This includes the range of potential and likely behaviors of relevant actors in response to joint force or others' activities.

5. The availability and capacity of specialized capabilities for the joint force to conduct OIE and information activities, to include those of mission partners.

6. The ability of the joint force to affect relevant actor behavior within the parameters of the mission. In other words, will the joint force be able to affect relevant actor behavior to the degree necessary and in sufficient time to support the achievement of the JFC's objectives?

7. The authorities and permissions available to the joint force to use specialized capabilities, to target specific relevant actors, and to undertake information activities.

8. The ability of relevant actors to attack or exploit the joint force's information, information networks, and information systems.

9. The ability of the joint force to protect its information, information networks, and information systems from relevant actor action and the resilience of those information networks and systems.

10. The ability of the joint force to manage and share friendly information to support effective decision making and C2 during operations, especially during multinational operations.

(d) **Determine and Analyze Operational Limitations.** Some operational limitations may arise due to the inherent informational aspect of military activities, the effects of which are not geographically constrained or limited to a joint force's intended audiences. The joint force cannot control the spread of information or its impact on audiences, within or beyond their specified JOA. This may restrict a commander's freedom of action if the informational aspect of a COA undermines higher-priority national objectives or negatively impacts the operations of other JFCs. Based upon their understanding of how information impacts the OE, information planners work with the other joint planners to develop a list of limitations related to relevant actors, the employment of specialized capabilities or conduct of information activities, and the use of specific themes and messages. Many of these limitations will be specified in authorities and permissions from higher headquarters.

(e) **Determine Specified, Implied, and Essential Tasks and Develop the Mission Statement.** The commander and staff review the planning directive's specified tasks and discuss implied tasks during planning initiation, then confirm the tasks during mission analysis. Information planners identify specified and implied tasks to understand how information impacts the OE, leverage information, and support decision making. Information planners identify other implied tasks based upon their analysis of the informational, physical, and human aspects of the OE and on an understanding of the relevant actors and how to affect their drivers of behavior. From the lists of specified and implied tasks, the commander and staff determine the essential tasks and use them to develop the mission statement.

(f) **Conduct Initial Force and Resource Analysis.** During mission analysis, the commander and staff team begin to develop a list of required forces and

capabilities necessary to accomplish the specified and implied tasks. Information planners contribute to this list by identifying those forces and capabilities required to understand how information impacts the OE, support human and automated decision making, and leverage information. In resource-constrained environments, military forces or capabilities may be unavailable or not readily available to meet all requirements. As part of their initial force and resource analysis, information planners should consider:

1. The lead time to deploy information forces and specialized capabilities into theater or direct support to the joint force from a home location.
2. The lead time to coordinate approval of information authorities and activities.
3. RFF or personnel with unique skills such as linguists, sociocultural experts, social media experts, experts in analyzing publicly available information, as well as experts on artificial intelligence and machine-learning.
4. Collaborating with mission partners who have information forces and specialized capabilities and the capacity to fill joint force resource gaps.
5. Planners evaluate appropriate requirements against existing or potential contracts or task orders to determine if a contracted support solution can meet the requirement.

(g) **Develop Military Objectives.** Each military objective establishes a clear goal toward which all the actions and effects of a LOO or LOE are directed. While military objectives commonly describe the condition and/or the relative position of the joint or enemy forces, the JFC may also express objectives as a particular behavior that the military operation will bring about. Information planners work with the rest of the staff to determine attainable behavioral goals that are based upon the analysis of the OE, including the previously identified potential behaviors in response to joint force or others' activities. Information planners use these objectives to develop measures of effectiveness (MOEs) and MOE indicators to assess how well the joint force leverages information. These include identifying and incorporating indicators of trending success or failure into the monitoring and assessment plan before finalization of the overall plan. Planners should keep in mind that it may take a considerable amount of time to observe the effects of information activities and cause and effect relationship may be difficult to assess.

(h) **Develop COA Evaluation Criteria.** Information planners help develop evaluation criteria that measure the relative effectiveness and efficiency of a COA to address threats and avoid or mitigate hazards in or through the IE. Potential evaluation criteria may include whether and how well the COA:

1. Aligns planned actions with strategic and operational mission narratives to establish the legitimacy of the joint force mission and actions with relevant actors.

2. Includes information activities focused on producing the desired behaviors in prioritized relevant actors.

3. Includes information activities that protect the joint force from adversary attempts to undermine the joint force narrative or the legitimacy of the joint force mission and actions (e.g., coordinated PA efforts to engage foreign and domestic publics, leadership outreach to mission partners, and HN military and civilian leadership).

4. Includes information activities that prevent, counter, and mitigate adversary or enemy attempts to undermine the joint force decision making and C2 (e.g., hardening of information systems against known enemy capabilities, building resiliency into C2 systems)

5. Identifies and accounts for the potential second- and third-order effects and potential risks to enduring strategic objectives (e.g., hardening of information systems against known enemy capabilities, building resiliency into C2 systems).

6. Accounts for the potential impacts on the joint force from the activities that resonate in and through the IE.

(i) **Develop Risk Assessment.** Information planners characterize the risk of obstacles or actions having effects in and through the IE that could preclude mission accomplishment. This includes actions that counter the narrative and indicate a “say-do gap” in joint operations. Information planners are responsible for carefully articulating this risk characterization so that commanders have a clear understanding of the potential benefits and dangers associated with information activities. Many of these impediments can be derived from an examination of friendly strategic and operational COGs and include, but are not limited to, the following:

1. Likelihood and impact of an adversary denying friendly C2 through technical means (e.g., EMSO or CO).

2. Likelihood and impact of allied or partner nation withdrawing support from a multinational operation.

3. Likelihood and impact of the collateral effects of joint force actions (e.g., civilian casualties, economic hardship, cultural offense) undermining the strategic or operational narrative and/or legitimacy of the joint force operation.

4. Likelihood and impact of adversary propaganda efforts undermining joint force strategic or operational narrative and/or legitimacy of the joint force operations.

5. Likelihood and impact of friendly force casualties undermining domestic support for joint force operations.

6. Likelihood and impact of international pressure causing cessation of joint force operations prior to strategic objectives being achieved.

See Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3105.01, Joint Risk Analysis, for additional information and guidance on risk determination.

(j) **Determine Initial CCIRs.** CCIRs identify key elements of information the commander identifies as being critical to timely decision making.

1. Information planners should consider the following as potential priority intelligence requirements (PIRs):

a. Intelligence required to resolve any remaining assumptions related to adversary actions or capabilities or unresolved assumptions regarding the IE.

b. Intelligence required to detect the existence of any obstacles or any adversary actions that were characterized during risk assessment as moderate or higher risk.

c. Intelligence about the pending or actual conduct of activities by opponents or other actors that will create effects in and through the IE that will likely impact the JFC's or strategic objectives (e.g., an opponent's announcement that they will withdraw forces from a contested area, a political announcement that would cause partner nations to doubt US or joint force resolve to continue operations, corruption in a supported government that would cause locals to oppose that government and the joint force).

2. Information planners focus on the following as potential friendly force information requirements (FFIRs):

a. Information required to resolve any remaining assumptions related to the availability and capabilities of friendly information forces and OIE units or of authorities and permissions to employ those capabilities or conduct information activities.

b. Any change in status of OIE units or specialized information forces' capabilities, to include MNF partners conducting information activities.

c. Any change in the authorities or permissions to employ specialized capabilities or conduct information activities.

d. Information on the planned or actual conduct of activities by other commands that will create effects in and through the IE that will likely impact the JFC's or strategic objectives.

e. Planned or actual activities by or related to mission partners that would undermine the composition or cohesiveness of the MNF (e.g., political

developments in a partner nation that could jeopardize continued support by forces from that nation, operations by the forces of one mission partner that are publicly opposed by another).

f. Degradation or loss of any communication capability resulting in the JFC's inability to C2 the joint force.

g. Loss of access to social media or other outlets the joint force is using to understand, inform, and influence relevant actors.

h. Loss of critical access point or other conduit the joint force is using to attack, exploit, or deny information, information, networks, and information systems of relevant actors.

(k) Prepare Staff Estimates

1. The information planners produce the information staff estimate in conjunction with OIE units and Service component information planners. That estimate includes the status and capabilities of OIE units or other forces tasked with leveraging information or elements that are critical to joint force protection of the joint force's information, information networks, or information systems. The information staff estimate includes an analysis of how information impacts the OE, as well as an assessment of how the inherent informational aspects of activities planned by each of the functional areas might impact the IE in ways to support or to undermine achieving the JFC's objectives. The information staff estimate will also identify additional capabilities to augment organic assets.

For a sample template of an information estimate, see Appendix B, "Information Staff Estimate Format."

2. The intelligence estimate includes an information section. This section should include relevant aspects of the IE, such as:

a. Inputs from capabilities, operations, and activities that gather operational information. These include, but are not limited to, CA, KLE, PA, MISO, OPSEC, JEMSO, COMCAM, space operations, and CO.

b. Those likely and dangerous transitions of enemy, adversary, or competitor behavior that challenge US objectives. This section enables planners to estimate the interests, intent, capability, capacity, and likely disruptive actions of relevant actors to support or counter USG interests.

For additional information on the intelligence estimate, refer to CJCSM 3130.03, Planning and Execution Formats and Guidance.

(l) Prepare and Deliver Mission Analysis Brief

1. Upon conclusion of the mission analysis, the staff, including information planners, will present a mission analysis brief to the commander.

2. A key portion of the information planners' input to the mission analysis briefing is the development of the operational mission narrative. The operational mission narrative will immediately follow the commander's intent in the final plan or order. The commander's intent describes the desired outcome, and the operational mission narrative communicates the "why," "how," and "by whom" of an operation. A well-crafted mission narrative and commander's intent provides coherence to military actions and activities and facilitates synchronization of communications and actions. Tactical units use the commander's intent and the operational mission narrative to develop a tactical or local narrative that lends continuity to operations and communications.

(3) Step 3—COA Development. A COA is a potential way to accomplish the assigned mission. After the mission analysis briefing, the staff begins developing COAs for analysis and comparison based on the commander's intent, operational mission narrative, restated mission, and planning guidance. A good COA accomplishes the mission within the commander's guidance, advances the narrative, provides flexibility to meet unforeseen events during execution, and positions the joint force for future operations.

(a) Information planners use their specific expertise to:

1. Identify ways land, maritime, air, space, cyberspace, and special operations forces contribute to each of the tasks of the information joint function.

2. Advise on how the joint force can leverage the inherent informational aspects of activities to create or shape the desired perceptions to achieve the commander's objectives.

3. Advise on how to integrate actions in the physical domains, IE (including cyberspace), and EMS to align with the operational mission narrative.

4. Identify threats, vulnerabilities, and opportunities in the IE.

5. Determine how to task-organize and employ OIE units and other information forces in support of objectives. This includes identifying how OIE will amplify or conceal physical actions in a manner that increases or decreases ambiguity.

6. Identify critical capabilities required to inform domestic, international, and internal audiences; influence relevant actors; and attack and exploit information, information networks, and information systems.

7. Identify any friendly information systems or segments of friendly information networks that need to be prioritized for defensive actions based on each COA.

8. Identify critical information the joint force needs to protect for each COA and recommend appropriate protection measures.

9. Determine communication channels that are most credible to and are most effective for reaching the selected audiences.

10. Identify how to integrate lethal and nonlethal actions required to create specific effects in and through the IE (e.g., destruction of a radio tower) into existing targeting and fires planning processes.

(b) Review objectives and tasks and develop ways to accomplish tasks. During COA development, planners review and refine objectives from the initial work done during the development of the operational approach. Information planners determine the tasks required to effectively leverage information to achieve the refined objectives. These objectives and tasks are assigned in plans or orders to joint force units, including OIE units (see Chapter VII, “Operations in the Information Environment,” for a discussion of OIE). COAs should include tasks to inform domestic and international, and internal audiences; influence relevant actors; and attack and exploit information, information networks, and information systems. See Chapter II, “Joint Force Uses of Information,” paragraph 7.c., “Leverage Information,” for a discussion of these tasks.

(c) Select and prioritize audiences, TAs, and targets. Information planners participate in the joint targeting process during COA development to identify and prioritize relevant actors with whom the joint force will interact. Relevant actors are categorized as audiences, TAs, or targets depending upon their relationship to a threat and the means with which the joint force will interact with them (i.e., whether through lethal or nonlethal engagement).

1. Audiences. Audiences are a broadly defined group that contains stakeholders and/or publics relevant to military operations. Audiences are not the enemy and do not directly perform a function for the enemy. KLE, PA, and CMO are examples of activities that use the term audiences to characterize the relevant actors selected for engagement. Information planners aid in selecting and prioritizing audiences to ensure activities are synchronized and deconflicted and to prevent or mitigate any negative effects caused by fires or other information activities.

2. TAs. A TA is an individual or group selected for influence. Individuals or groups are designated as such when a change in their behavior is necessary to achieve the commander’s objectives. TAs will sometimes also meet the criteria of a target if they perform a function for a threat, whether they do so knowingly or not, willingly or unwillingly. In those cases, TAs are included on one of the joint target lists to be prioritized, vetted, and approved in accordance with JFC priorities; legal, political, and operational constraints; rules of engagement; collateral damage restrictions; political considerations; and operational requirements.

3. Targets. A target is an entity or object that performs a function for the threat considered for possible engagement or other action. A TA may be a target if it is the adversary or performs a function for the adversary. A target's importance derives from its potential contribution to achieving a commander's objective(s) or otherwise accomplishing assigned tasks. Offensive military activities (e.g., electromagnetic attack, cyberspace attack, MISO) should be coordinated and deconflicted within the joint targeting process. Information planners participate in the targeting working groups and boards to nominate targets, identify targets for inclusion in the joint restricted fires list, and evaluate targets for their psychological impact on relevant actors. The traditional methodology of identifying target systems, sets, components, and their critical elements remains valid for OIE. Some capabilities used for OIE may require long lead time for development of the JIPOE and release authority and should be identified as early in the target process as possible.

(d) Identify the sequencing (simultaneous, sequential, or a combination) of actions for each COA. Understand which resources become available and when during the operation or campaign. Resource availability will significantly affect sequencing operations and activities. Sequencing of inform, influence, and attack tasks rely on the relevance of the information in relation to the timing of an event. Any gap between publicized information and performance of an activity has the potential to undermine the intent of the activity and negatively affect the achievement of objectives. Information planners carefully consider how the sequencing of activities will impact the inherent informational aspects of each COA. This includes consideration of how information activities will be synchronized with other activities to enhance the effectiveness of the COA (e.g., synchronizing jamming against an IADS in support of air interdiction). The timing and synchronization of activities of each COA should consider how it can pre-empt, undermine, or counter adversary and enemy use of narratives, especially those that convey misinformation or disinformation. This is critical due to the extreme difficulty to change minds or beliefs, even when presented with facts and evidence once an audience has been influenced by misinformation or disinformation. Therefore, the goal is to provide accurate and useful information to relevant actors in a timely manner to increase its credibility and relevance. Information planners can advise on how each COA can communicate information in a timely fashion, multiple times, and from multiple sources to create the desired effects.

(4) Step 4—COA Analysis and Wargaming. COA analysis is the process of closely examining potential COAs to reveal details that enable the commander and staff to tentatively evaluate COA validity and identify the advantages and disadvantages of each proposed friendly COA. Wargaming is a primary means for COA analysis. Wargames are representations of conflict or competition in a synthetic environment, in which people make decisions and respond to the consequences of those decisions.

(a) During COA analysis and wargaming, information planners examine how well each COA leverages information to achieve objectives. Wargaming helps the staff to visualize the flow of the operation and, in doing so, facilitates understanding the effects of the joint force's leveraging of information. During wargaming planners also

examine the extent to which joint force activities align with and support JFC's operational mission narrative. Information planners help examine friendly and adversary information activities (i.e., those activities that inform audiences; influence foreign relevant actors; and attack and exploit relevant actor information, information networks, and information systems) to determine their potential effects in relation to the objectives. To the extent possible, those personnel or organizations tasked to conduct such activities participate in the wargaming process. Wargaming might identify activities that were previously not identified. During COA analysis and wargaming, information planners help the staff:

1. Determine the likelihood that joint force activities will affect relevant actor behavior. This includes consideration of how relevant actors are likely to react to information activities and the inherent informational aspect of physical activities.

2. Determine the relative importance of relevant actors and identify the potential emergence of new relevant actors.

3. Identify high-value targets related to inform, influence, attack, or exploit activities.

4. Identify decision points related to the joint force's leveraging of information to change or maintain perceptions, attitudes, and other drivers of relevant actor behaviors.

5. Identify how the joint force reacts to threats, vulnerabilities, and opportunities in the environment.

6. Identify and recommend adjustments to information tasks conducted by information forces, including OIE units.

7. Recommend adjustments to task organization of joint force elements to better support leveraging information and the inherent informational aspects of activities.

8. Identify and provide time, space, and purpose input for synchronization matrices or other decision-making tools.

9. Identify tasks that leverage information for branches and sequels.

10. Identify PIRs and FFIRs.

11. Refine information concept of support (the description of how information will support the CONOPS).

12. Refine sequencing and timing of information activities.

13. Refine risks associated with joint force use and leveraging of information.

14. Review and update the information estimate (see Appendix B, “Information Staff Estimate Format”) from applicable OPLANs and concept plans.

(b) COA analysis and wargaming benefits from the participation of red teams, green cells, and white cells. Because they bring a different perspective into COA analysis and wargaming, these elements help joint planners reduce mirror-imaging and better understand and evaluate the potential actions and reactions of relevant actors. SMEs for red teams, and for green and white cells may include multinational partners, behavioral scientists, and cultural anthropologists. If not resident to the core planning staff, these experts may be available through reachback support.

(5) **Step 5—COA Comparison.** COA comparison is both a subjective and objective process, whereby COAs are considered independently and evaluated/compared against a set of criteria that are established by the staff and commander. COA comparison starts with all staff elements analyzing and evaluating the advantages and disadvantages of each COA from their respective viewpoints. Each of the COA evaluation criteria should contain information considerations. During mission analysis, information planners helped develop the evaluation criteria used in COA to measure the relative effectiveness and efficiency of a COA to address threats and avoid or mitigate hazards in or through the IE. How well the joint force uses information and leverages information may indirectly affect the rating of that COA evaluation criteria. For instance, if “speed of movement” is specified as an evaluation criteria and a COA is relying on deceiving an enemy decision maker to facilitate unimpeded movement, that COA is dependent upon the ability of the joint force to leverage information to affect behavior. If only one of multiple COAs is relying on deception, then the ability of the joint force to leverage information to affect behavior will impact the rating of that criteria for that one COA more significantly than the others.

(6) **Step 6—COA Approval.** In this JPP step, the staff briefs the commander on the COA comparison and the analysis and wargaming results and provides the commander with a recommended COA. The commander combines personal analysis with the staff recommendation, resulting in a selected COA. It gives the staff a concise statement of how the commander intends to accomplish the mission and provides the necessary focus for planning and plan development. The information planner helps the staff refine the commander’s COA selection into a clear decision statement, then completes the commander’s estimate. The commander’s estimate provides a concise statement of how the commander intends to accomplish the mission and provides the necessary focus for campaign planning and contingency plan development. The commander’s estimate will include the refined commander’s intent along with the commander’s operational mission narrative.

(7) **Step 7—Plan or Order Development.** This final JPP step includes development of the CONOPS and publication of a plan or order. During plan or order

development, the staff further develops and refines component missions and tasks that specify how the joint force will use information and leverage information to achieve objectives. The final plan or order will assign those missions and tasks to OIE units and other information forces.

Intentionally Blank

CHAPTER V EXECUTION

1. Introduction

a. Chapter IV, “Operational Design and Planning,” explained how the joint force institutionalizes the use and leveraging of information as a functional element of maneuver in the design and planning of operations. This chapter discusses the context in which the joint force will conduct operations and the essential elements necessary to incorporate information into execution.

b. Execution puts a plan into action by applying the power of the joint force to accomplish the mission and adjusting operations based on changes in the situation. Commanders and staffs use situational understanding to assess progress and make execution and adjustment decisions. They apply all available joint force abilities to seize, retain, and exploit the initiative to gain and maintain a position of relative advantage. Commanders gain an operational advantage through their ability to deliberately persuade or coerce desired perceptions, attitudes, and other drivers of behavior to achieve enduring outcomes with our partners, competitors, or adversaries. This advantage contributes to their freedom of action and ability to affect operational tempo.

2. Execution in Context

Joint operations span the competition continuum from recurring cooperative activities to sustained combat operations in armed conflict. The application of informational power expands commanders’ range of options for action across the competition continuum. The application of informational power may be the primary option available to a JFC during long-duration cooperation and competition short of armed conflict, where the use of physical force is inappropriate or restricted.

For a discussion of the competition continuum, see JP 1, Volume 1, Joint Warfighting, and JP 3-0, Joint Campaigns and Operations.

See Chapter II, “Joint Forces Uses of Information,” paragraph 4, “Informational Power,” for more discussion of informational power.

3. Essential Elements for Incorporating Information into Execution

At its most basic level, execution involves synchronizing activities to maximize their combined effects during the conduct of operations; monitoring those activities and the effects they have on the OE; and adjusting activities based upon threats, vulnerabilities, and opportunities in the OE. The JFC focuses on synchronizing, monitoring, and adjusting all joint force activities (i.e., not just information activities) so they have the desired effects in and through the IE and support achievement of joint and national objectives. The dynamic nature of the IE makes it vital that the JFC have the organizations, processes, and tools in place to rapidly recognize the informational aspects of activities and adapt joint

force activities in response to failures or to exploit successes in and through the IE. The following are essential elements that facilitate that rapid adaption.

a. **Organization.** The JFC modifies current or establishes new command and staff structures, as necessary, to facilitate joint force unity of effort to use and leverage information. This includes the option of establishing an OIE unit with the personnel, authorities, and other resources to conduct OIE. This requires an overarching strategy to gain operational advantage through the use of information and synchronizing the execution of that strategy between the command, subordinate units, and supporting or related operations of component commanders.

See Chapter III, “Unity of Effort,” for a discussion of staff organizations and the component command for information. See Chapter VII, “Operations in the Information Environment,” for a discussion of OIE units.

b. **Monitoring and Analyzing for Effects In and Through the IE**

(1) Monitoring and analysis comprise the observation and evaluation of how information impacts the JFC’s OE, how joint force activities affect relevant actors, and how those activities resonate in and through the IE to affect other JFC’s OEs. Monitoring and analysis contribute to maintaining situational awareness for the command and are facilitated by sharing information and knowledge. They include observing and evaluating the informational, physical, and human aspects of the OE for potential threats, vulnerabilities, and opportunities (to include a nuanced view of relevant actors) that could impact the JFC’s decisions concerning mission requirements.

(2) The JFC may establish and resource an information CFT with the means to monitor and recommend adjustments to joint force operations to align them with objectives and the strategic and operational narratives. This forum provides visibility on the effects of joint force activities that impact the IE and presents proactive options to the JFC for the leveraging of information to affect behavior. The information CFT is integrated into the JFC’s battle rhythm to provide more accurate and timely situational awareness and promote more effective use and leveraging of information.

Refer to Chapter III, “Unity of Effort,” for more information on the information CFT.

c. **The Synchronization Matrix.** An information synchronization matrix, built around the CONOPS, contains the phasing of the operation and enables planners to graphically display the activities, linked to the scheme of maneuver, that leverage information to affect behavior and impact the OE. The matrix displays the mechanics of physical movement but, more importantly, reveals how the informational aspects of the operations are knitted together with other functional elements of joint maneuver to deliberately show or hide joint force activities or intentions. The body of the matrix contains critical tasks, arrayed in time and linked to responsible elements for execution. Joint force planners may use a matrix to display progress against actual execution and recommend adjustments as needed. It is important for the matrix to identify when tasks

are executed and when effects are required since they often do not align. For example, MISO messages may be disseminated during a certain window, but the desired effect may happen much later. The synchronization matrix also helps planners identify potential gaps, develop options to mitigate those gaps, and respond to a changing OE.

d. **CCIRs.** Information planners update the critical information requirements to provide the JFC with an understanding of how information impacts the OE; an awareness of the threats, vulnerabilities, and opportunities in the IE; and the status of organizations critical to supporting human and automated decision making and leveraging information.

Refer to Chapter IV, “Operational Design and Planning,” for a discussion of CCIR relevant to the joint force use and leveraging of information.

e. **The Narrative.** The narrative can be thought of as a unifying story that acts as an information control measure to avoid conflicting messages and promote unity of effort. This is analogous to control and coordination measures used for maneuver and movement control, airspace coordination, and fire support coordination. The JFC and staff monitor the effects in and through the IE of the activities of the joint force to ensure those activities support the narrative.

f. **Information and KM.** IM and KM ensure users are aware of and can access critical information for decision making and enables shared understanding. During execution, IM and KM facilitate synchronization, monitoring, and direction of activities. Effective IM and KM are essential for staying inside the enemy’s decision-making cycle. Combined with effective planning, IM and KM help commanders anticipate enemy actions and develop branches, sequels, or adjustments.

For additional details on KM and IM, refer to Chapter II, “Joint Force Uses of Information,” paragraph 7.b.(1)(b), “KM and IM,” and to JP 3-33, Joint Force Headquarters.

g. **The Information Staff Estimate.** The information planning cell is responsible for the information staff estimate. The information staff estimate is a continual evaluation of how factors related to the IE impact the planning and execution of operations. The purpose of the information staff estimate is to inform the commander, staff, and subordinate commands on how information can be used to support mission accomplishment. The estimate helps feed the commander’s estimate and contributes to the JFC’s common operational picture of the OE for planning, mission coordination, and assessment of all operations. The information planning cell on the JFC’s staff produces this consolidated estimate as an overview of all capabilities and activities available to perform tasks related to the information joint function. It includes the analysis of the informational, physical, and human aspects of the environment; the status of friendly OIE units and information forces and their activities; and an assessment of adversarial capabilities and intent. See Appendix B, “Information Staff Estimate Format,” for a sample format.

Intentionally Blank

CHAPTER VI ASSESSMENT

1. Introduction

This chapter is about determining the effectiveness of the joint force's use of information and leveraging of information to achieve the commander's objectives. Assessing the use and leveraging of information allows the JFC to appreciate whether, and to what extent, those efforts are helping to achieve objectives and gain/exploit information advantage. Assessment of joint force information activities is a continual and cyclical process.

- a. Whether inform, influence, and attack activities are driving competitors, adversaries, or enemies to the desired actions.
- b. Whether shared understanding activities contribute to achieving unity of effort.
- c. Whether activities to protect information, information systems, and information networks are contributing to making decisions.
- d. Whether protect actions shield joint force personnel from malign influence.

For more details on assessment, see JP 3-0, Joint Campaigns and Operations, and JP 5-0, Joint Planning.

2. Requirement for Assessment

a. Assessment of operations and activities is key to the commander's decision cycle, helping to determine the results of actions in the context of overall mission objectives and providing recommendations for refinement of future plans. Assessing the joint force's use and leveraging of information in joint operations provides data and analysis to inform the commander on how effectively the joint force is able to understand how information impacts the OE, support human and automated decision making, and leverage information to achieve objectives.

b. Embedded in all military operations is the requirement to provide operational reporting to all echelons of command with essential information on the planning, initiation, termination, and results of military operations. Additionally, some operations (such as CO and MISO) have quarterly and annual reporting required by Congress. This operational reporting impacts future decisions, efforts, and resources. Operational reporting provides the data required to support other analyses and assessments.

c. Staff estimates are continually updated based on changes in the situation. Operation assessment provides the means to maintain running staff estimates for each functional area. The staff estimates identify available CCMD capabilities and anticipated shortfalls that may limit the ability to support the proposed friendly COAs. They are the link between

planning and execution and support continuous assessment and can help commanders decide to adapt plans or shift resources based upon the intelligence and other staff estimates, including the information staff estimate (refer to Appendix B, “Information Staff Estimate Format”), as well as input from other mission partners.

3. Challenges Assessing Information in Joint Operations

a. Distinguishing between correlation and causation makes information activity assessment difficult. Analysts should approach assessment with open minds and determine whether correlation, causality, or a combination of the two is the appropriate approach for specific MOEs. This approach provides insights to the likelihood of particular events and effects given certain criteria in terms of conditions and actors in the OE. When assessing information in joint operations, evidence has shown that correlation between indicators and events has proven more accurate than efforts to establish concrete cause and effects relationships. This is especially true when assessing public opinion or human behavior. Unforeseen factors can lead to erroneous interpretations, for example, a traffic accident in a foreign country involving a US Service member or a local civilian’s bias against US policies can cause a decline in public support, irrespective of otherwise successful operations. Incorrect assumptions about causality in a complex system can lead information planners to incorrect conclusions that undermine planning for future operations. This exposes the assessment to potential discredit, especially if counter-examples exist.

b. Other factors that complicate the assessment of information activities include:

(1) Intelligence assets may not have the ability to directly gather the necessary data on a relevant actor in a timely manner.

(2) Logistical challenges related to capturing accurate data, particularly in hostile or uncertain environments.

(3) Operational tempo.

(4) Rapidly changing conditions that affect the accuracy and volume of data that is able to be collected.

(5) Cognitive biases that influence accuracy.

(6) Requirement for resource-intensive continual and cyclical assessments.

(7) Incomplete data.

(8) Lack of universal measures and indicators of data used for assessment.

(9) Complexity of assessing joint operations may also require specialty expertise, assets, and capabilities that exceed the organic capability of the command.

c. It is possible for the planner to fall prey to perfectionism. Given the inherent biases and the limitations of measurement and collection tools, planners seek to reduce uncertainty about the value being measured as opposed to seeking perfect accuracy or precision. The information planner should articulate any challenges or obstacles encountered so the commander understands the relative reliability of the assessment, such as restricted access to populations for data collection, small sample size, incomplete data, and changes in collection methods.

4. Organizing for Assessment

a. Organizing for assessment involves identifying the appropriate data needed to assess progress during the operation and whether that data can be measured at all. Typically, data refers to facts or information used to calculate, analyze, or plan. In the case of assessment, the appropriate data should provide the basis for identifying changes in conditions as they relate to specific plan outcomes.

b. Organizing for assessment also impacts staff organization. Assessment of information in joint operations is commander led; it is supported by, but not delegated to, a staff activity. The way the staff is organized for assessment is a commander's prerogative; however, it is critical that the assessment staff be embedded throughout the planning process. Refinement and specification of objectives are integral parts of the planning process. Three potential approaches for organizing for assessment are:

(1) Special staff section. In this approach, the assessment element reports directly to the commander, via the COS or deputy commander. In such an organization, information professionals could advise lead planners on the use and leveraging of information, in addition to their role in the assessment of information LOEs. Advantages of this approach may include increased access to the commander and visibility on decision-making requirements, as well as an increased ability to make recommendations to the commander as part of the assessment process. Disadvantages may include being isolated from the other staff sections, thereby not having staff support and not having access to the information being collected and monitored across the staff.

(2) Separate staff section. In this approach, the assessment element is its own staff section, akin to plans, operations, intelligence, logistics, and communications. In a separate staff section, information professionals would need to take proactive measures to ensure full participation in all planning events and avoid stovepiping. The advantage of this approach is that it legitimizes assessment as a major staff activity equivalent with the other staff functions and enables the assessment team to participate in staff coordination and activities as co-equals with the other staff sections. A disadvantage to this approach is that it has the potential to create stovepiped assessment efforts without full collaboration for a whole-of-staff assessment.

(3) Integrated in another staff section. In this approach, the assessment element is typically integrated into the operations or plans sections and the assessment chief reports to the plans chief or the operations chief. Integrating information planners into an

operations or plans section could involve them being dedicated to specific planning efforts. The advantage of this approach is that it tends to create close ties between the assessment team and either the plans or operations teams, but a significant disadvantage is that it limits the number of information planners who can contribute to the assessment products for that specific planning effort.

(4) Integrating assessment into the planning effort is normally the responsibility of the lead planner, with assistance across the staff. The lead planner understands the complexity of the plan and decision points established as the plan develops. The lead planner also understands potential indicators of success or failure. It is the information planner's responsibility to support the lead planner with perspective on information's role in the overall plan.

(5) When conducting highly classified operation assessments, such as during MILDEC operations, special consideration is given to assessments with limited staff access. Assessment staff provides guidance to these special access elements to standardize timing and products with other operation assessment efforts.

(6) As a plan becomes operationalized, the overall assessment responsibility typically transitions from the lead planner to the J-3. The information lead provides the necessary information and analysis to guide the assessment and recommendations for implementing specific changes to better accomplish the mission.

5. Assessment Process

Assessments of information in joint operations are conducted in accordance with the assessment process shown in Figure VI-1. The assessment plan for a campaign integrates products from a range of strategic objectives, each encompassing its own set of intermediate objectives and desired conditions, subordinate operations, subordinate plans (i.e., country-specific security cooperation sections/country plans, contingency plans not in execution, ongoing operations, directed missions). Operational-level assessment must account for progress or setback of multiple operational-level objectives within the operation or campaign.

a. Step 1—Develop Assessment Approach

(1) The first step is to develop the assessment approach. The assessment approach, which eventually becomes the assessment plan (refer to Figure VI-2), is a description of the specific information needed to monitor and analyze desired effects created and progress toward achieving the objectives. Development of the assessment approach begins during the first step of the JPP as the command develops its operational approach and identifies the desired outcomes. The staff begins to develop the assessment approach by identifying and establishing the appropriate framework and structure needed to assess progress during the operation or campaign. Information planners contribute to developing the assessment approach by participating in the JIPOE process through the analysis of the IE (see Chapter IV, "Operational Design and Planning," paragraph

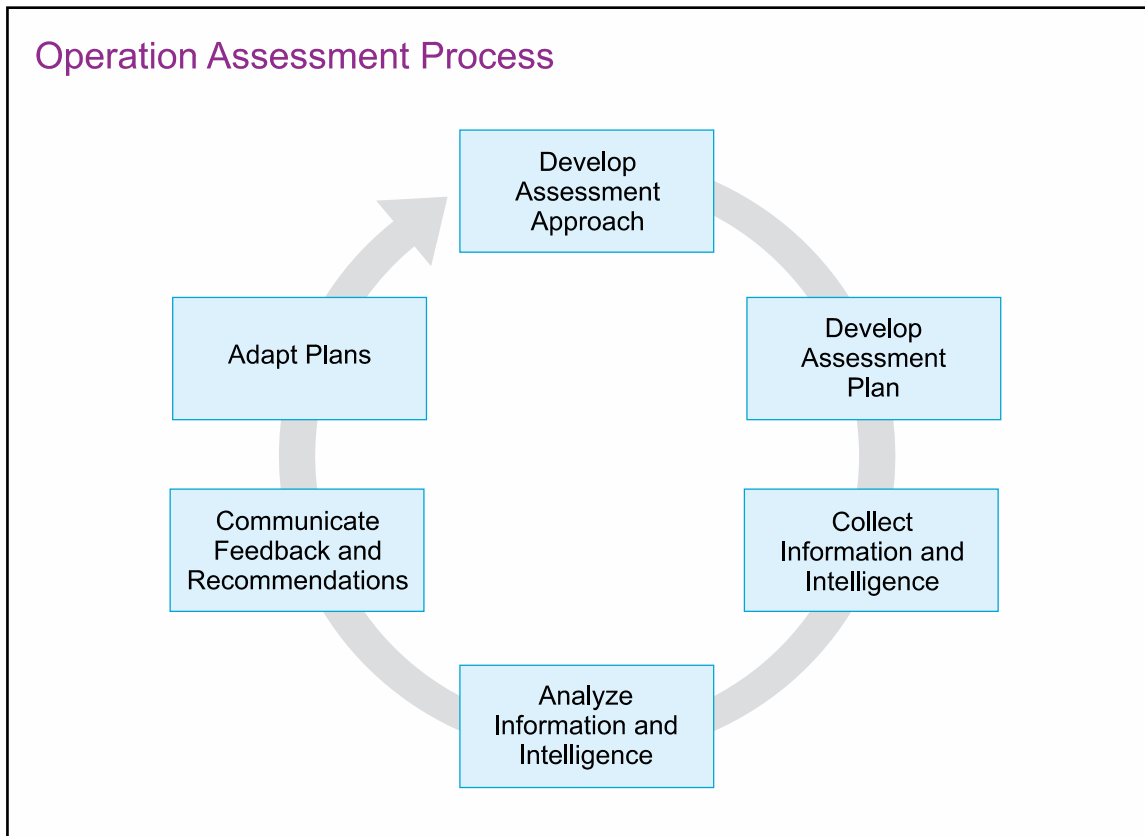


Figure VI-1. Operation Assessment Process

3.b.(3)(a), “Characterize the human, informational, and physical aspects of the OE”) and by advising on the best approach for measuring the impact of joint force activities on the IE.

(2) As part of developing the assessment approach, information planners develop a framework for assessing the inherent informational aspects of joint force activities and OIE. This framework includes collection and reporting responsibilities. The assessment plan continues to mature through plan development. The assessment plan describes how to answer three questions: What indicates progress toward the desired outcomes? What data is required? Who or what is best postured to provide that information?

(3) During initial planning, the joint force uses information from intelligence assessments and estimates from the JIPOE process, as well as specific information and intelligence requirements identified during the development of the assessment approach to form the initial assessment baseline. The baseline is necessary for identifying changes in conditions and serves as a reference point for comparison, enabling an assessment of the way in which activities create desired effects. This typically requires assessment planning and initiation of data collection prior to commencing the assessed operation. It is not always imperative that baseline data be quantitative. Sometimes, qualitative baseline data (such as data from focus groups) can provide a sufficient baseline. However, when qualitative data collection is used, there should be a predetermined plan to systematically code and/or quantify information in order to measure change over time. The baseline

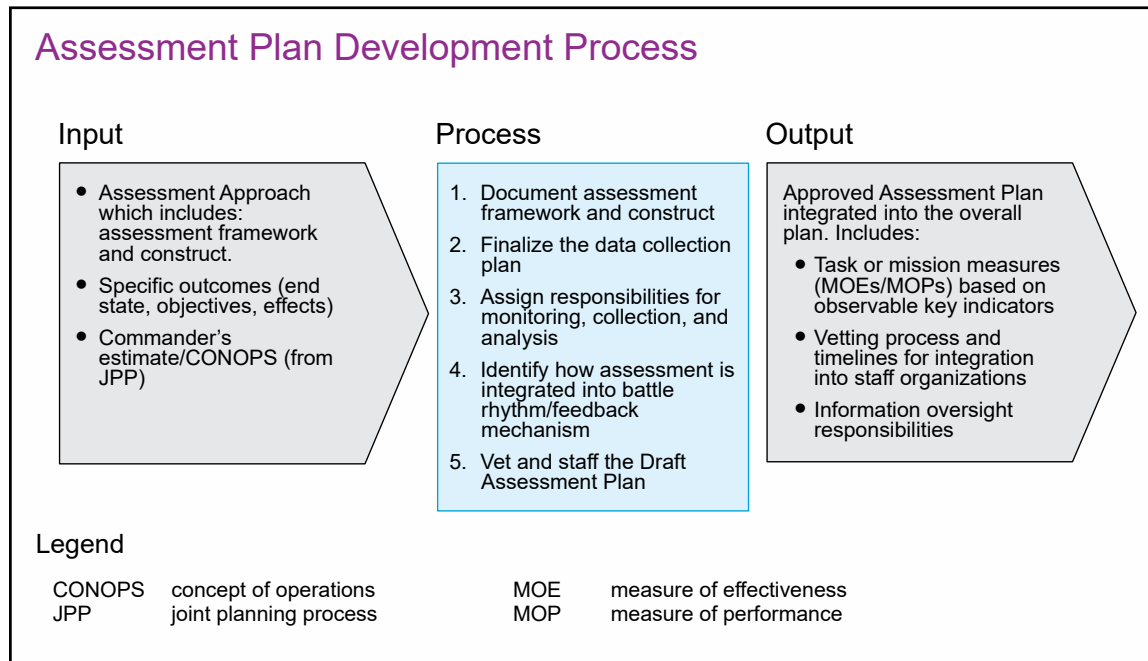


Figure VI-2. Assessment Plan Development Process

enables the commander and staff to set goals for desired rates of change within the OE and establish thresholds for success and failure. This focuses information and intelligence collection on answering specific questions relating to the plan. This will also capture the constellation of narratives in the IE, which ones resonate with whom and why, as well as how the joint force's hierarchy of narrative can compete.

b. Step 2—Develop Assessment Plan

(1) Early integration of assessments into plans is paramount. One of the first things that happens during planning is to ensure the objectives to be assessed are clear, understandable, and measurable. Equally important is to consider, as part of the assessment baseline, a description of the conditions within the OE at the time the baseline was established to help account for conditions outside of operations that may impact the assessment of the assigned tasks (e.g., statistics on the availability and usage of Internet in the region, literacy rates). Assessment products portray a progression from the baseline toward accomplishing a task, creating an effect, or achieving an objective.

(2) Developing and refining the assessment plan is concurrent and complementary throughout joint planning and modified during execution, if necessary. This step overlaps with the previous step during identification of the objectives and effects. Developing the assessment plan is a whole-of-staff effort and should include other key stakeholders to better shape the assessment effort. The assessment plan should identify staff or subordinate organization responsibilities for monitoring, collecting, and analyzing information and developing recommendations and assessment products as required. Requirements for staff coordination and presentation to the commander should also be included in the plan and integrated into the commander's decision cycle and the

command's battle rhythm. The information CFT is a stakeholder in the coordination of the assessment plan and serves as a cross-functional conduit to develop, implement, and consolidate assessments on the command's approach to synchronizing communications in support of JFC's objectives.

(3) When assessing joint force efforts to leverage information to affect behavior, it may take some time for the full effect of the activity or activities to be experienced. When assessing tasks and activities that leverage information, there are three likely outcomes. First, the message or action is not seen, heard, or experienced by the designated recipient or targeted system. Second, the desired recipient or targeted system disregards the message or activity. Third, the recipient or targeted system internalizes or processes the message or activity to some degree. Outcome variability requires the assessment process to both determine results and to feed back into the iterative process of re-engagement until the desired effect is created.

(4) When developing an assessment plan dealing with complex open systems, identifying and clearly articulating an expected change greatly aids in understanding task and objective, cause and effect relationships. Since the IE is an extraordinarily complex and open system, information planners can help the assessment team determine the interrelationships between tasks and objectives and between cause and effect for information LOEs.

(5) Mapping the expected change provides the clear, logical connections between activities and desired outcomes by defining intermediate steps between the current situation and the desired outcome. Mapping the expected change also assists in the development of MOEs and measures of performance (MOPs). It should include clearly stated assumptions that can be challenged for correctness as activities are executed. The ability to challenge assumptions in light of executed activities enables the joint planner to identify flawed connections between activity and effects, incorrect assumptions, or the presence of variables that are outside of the joint force's control and can influence the outcome causing a spurious association between joint force's actions and the effect. The example that follows shows:

(a) Logical connection between activities and effects. Activity: training and arming local security guards. Effect: increased ability to resist insurgents.

(b) Clearly stated assumptions; increased ability and willingness to resist leads to an increase in security in the locale; increased security leads to increased perceptions of security.

(c) Intermediate steps and points of measurement; MOPs regarding training activities; MOEs regarding willingness to resist; MOEs regarding increased local security. MOPs regarding number of local security guards armed and trained.

(6) This expected change shows a logical connection between activities (e.g., training and arming locals) and effects (e.g., increased stability). Even clearly stated

assumptions can be challenged if they are determined to be incorrect. Further, those activities and assumptions suggest obvious things to measure, such as performance of the activities and the resulting effect. They also suggest measurement of more subtle elements of all the intermediate logical nodes such as capability and willingness of local security forces, change in security, change in perception of security, change in participation in local government, and change in governance. Better still, if one of those measurements does not yield the desired result, the joint planner will be able to ascertain where in the chain the logic is breaking down, which hypotheses are not substantiated. The joint planner can then modify the expected change and the activities supporting it and continue to progress toward the objectives. Such an expected change might have begun as something quite simple: training and arming local security guards should lead to increased stability. But more is needed for building assessments. Stopping there would suggest only the need to measure the activity and the resulting effect and leaves a huge, assumptive gap. If training and arming security guards goes well, but stability does not increase, there will be no apparent reason why. To begin to expand on a simple expected change, the information planner should determine cause and effect. How might “A” lead to “B”? (i.e., in this case, how would training and arming security guards lead to stability?) A thoughtful answer to this question usually leads to recognition of another node to the expected change. If needed, the question can be asked again relative to this new node, until the expected change is sufficiently articulated.

(7) Circumstances on the ground might also require the assumptions in an expected change to be more explicitly defined. For example, using the expected change articulated in the above example, the joint planner might observe that, in successfully training and arming local security guards, they are better able to resist insurgents, leading to an increased perception of security, as indicated by increased traffic in local markets and other outdoor locations. However, participation in local government, as measured through voting in local elections and attendance at local council meetings, has not increased. The existing expected change and associated measurements illustrate where the chain of logic is breaking down (i.e., somewhere between perceptions of security and participation in local governance), but it does not (yet) tell why that break is occurring. Adjusting the expected change by identifying the incorrect assumption or spoiling factor preventing the successful connection between security and local governance will also help improve achievement of the objective.

(8) The assessment plan should also include a plan for how data will be analyzed and include specific statistical analyses, if applicable. The number of research questions/MOEs to be measured, the predictive variance in a TA, and data analysis will help determine how many responses or data points are required.

c. Step 3—Collect Information

(1) Well-developed MOEs serve as a foundation for development of intelligence requirements. To operationalize assessments, a collection management plan is critical. It is imperative that the data collected be tied to the assessment of MOEs. A collection plan is the integration of intelligence requirements with the assigned tactical, theater, and

national intelligence sources and other resources used for collection. This step also serves as a decision point for staff planners (including information planners). Not every intelligence requirement will be answered by the IC; therefore, planners should consider collaborating with other sources of information, to include DOS, the Department of Homeland Security, other USG departments and agencies, and academia. Information planners use publicly available information, surveys, polls, and other research to gather information and intelligence for MOEs.

(2) During preparation, for those operations not yet in execution, the joint force should continue to collect information in accordance with the data collection plan or as directed. Information planners will provide updates on changes in the IE. Analysis of this new information could result in changes to the operational approach, objectives, or planned tasks within the current plan.

(3) During mission execution, the joint force uses the data collection plan and defined reporting procedures to gather information about the OE and the joint force's actions as part of normal C2 activities. Typically, staffs and subordinate commands provide information about plan execution on a regular cycle through specified battle rhythm events. Intelligence staffs continually provide intelligence about the OE and operational impact to support the collective staff assessment effort. Information planners contribute to that support by monitoring activities and operations to determine progress towards achieving objectives, especially objectives for OIE. Planners monitor the threat and friendly situations to track accomplishment of information tasks, determine the effects of leveraging information, and detect and track any unintended consequences. Information planners work closely with the intelligence cell, intelligence staff officer, and information CFT representatives to provide a running assessment of the effectiveness of threat information efforts and keep the operations staff officer and various integrating cells informed. In accordance with the assessment plan, assessment considerations may help the planning, operations, network communications, and intelligence staffs when determining the presence of decision point triggers and other mission impacts across the staff.

d. Step 4—Analyze Information and Produce Intelligence

(1) To identify trends and changes, it is necessary to isolate, from the data, those differences that are the result of observable and predicted changes in the system from noise or normal variation in the indicators being collected. Analysis of data seeks to identify positive or negative movement or stagnation toward achieving objectives.

(2) While individual staff elements may be responsible for analysis within their functional area, the staffing and vetting process enables the assessment to develop coherent, holistic assessment products, including recommendations resulting from the individual analyses. As the entire staff conducts analysis of the OE, the information staff focuses on the informational attributes. This analysis occurs when planning for an operation begins or, in some cases, prior to planning for an operation (e.g., during routine analysis in support of combatant command campaign plan [CCP] activities). It is a required step for viable planning and provides necessary data for, among other things, development of MOEs,

determining potential TAs and targets, and baseline data (e.g., status of the potential TAs and targets, attitudes of the local populaces) from which change can be measured. Analysis is conducted by interdisciplinary teams and staff sections. The primary product of this step is a description of the informational, physical, and human aspects of the OE.

(3) Analysis of the OE identifies key functions and systems within it. The analysis provides the initial information to identify decision makers (human), factors that guide the decision-making process (informational), and infrastructure that supports and communicates decisions and decision making (physical).

(4) Gaps in the ability to analyze the OE and gaps in required information are identified and transformed into intelligence requirements and requests, RFFs and/or augmentation, and requests for support from external agencies. Technological, cultural, and infrastructure changes, regardless of their source or cause, can impact the informational aspects within a dynamic OE. Once the initial analysis is complete, periodic analyses should be conducted to capture changes and update the analysis for the commander, staff, other units, and mission partners. Much like a running estimate, the analysis of the OE becomes a living document, continuously updated to provide a current, accurate picture.

(5) If available, personnel trained or qualified in statistical analysis techniques should conduct data analysis. Analysis can be done outside the operational area by leveraging reachback capabilities. Nonstatistical comparisons (e.g., average rating of United States at baseline, time 1, and time 2) and graphs can also be presented, although limitations in interpretation of significance should be discussed. One of the most important factors for analysis is that it is conducted in an unbiased manner. Assessment data is analyzed and the results are compared to the baseline measurements and updated continuously as the staff continues its analysis of the OE. These comparisons help the staff determine whether the OE has changed and, if so, the degree and area of that change. These changes are indications of effects on or in the OE and help determine whether progress is being made toward achieving objectives. Assessment remains an iterative process.

(6) Military operations are inherently human endeavors. Analysts use both quantitative approaches (e.g., content analysis, descriptive statistics) and qualitative approaches (e.g., interviews, temperature maps) to assess the psychological effects of military operations. Military and nonmilitary SMEs should validate data quality and its appropriateness to the phenomena and answers being sought.

(7) Both qualitative and quantitative approaches require a sound statistical approach and expert interpretation to provide meaningful and accurate assessments. Even when data is collected and analyzed by trained personnel, errors can occur (e.g., unrecognized bias resulted in an incorrect cause and effect determination, errors in translation skewed the data). Transparency in the assessment process is vital to success. When problems or errors are found in the data, feedback about what occurred and where adjustments are necessary is reported, as appropriate. This is crucial as such feedback is critical to adjusting processes to avoid further issues.

e. Step 5—Communicate Feedback and Recommendations

(1) The staff may be required to develop assessment products, which may include summary reports and briefings, containing recommendations for the commander based upon the guidelines set forth in the assessment plan. Discussing assessment findings within the context of the commander's guidance is the most critical step in developing assessment products. Regardless of quality and effort, the assessment process is useless if the communication of its results is deficient or inconsistent with the commander's personal style of digesting information and making decisions.

(2) Assessment results enable staffs to ensure tasks stay linked to objectives and objectives remain relevant. They provide opportunities to identify capability shortfalls and resource issues that may be impeding effectiveness. These results provide information to agencies outside of the command or chain of command. The primary purpose of reporting the results is to inform the command and staff concerning the progress of objective achievement, create effects in the OE, and enable decision making. The published assessment plan, staff standard operating procedures, battle rhythm, and orders are documents in which commanders can dictate how often assessment results are provided and the format in which they are reported. The staff reports progress and makes recommendations for plan adjustments, as necessary. The assessment team ensures that organizational procedures are established for capturing the commander's decisions and guidance resulting from assessment results and the actions taken (e.g., increased media coverage, decrease in shows of force).

f. Step 6—Adapt Plans for Operations, Campaigns, and Assessment

(1) Once feedback and recommendations have been provided, commanders typically direct changes or provide additional guidance that dictates updates or modifications to operation/campaign plans. There may also be implications of those decisions or guidance impacting the need to modify the assessment plan.

(2) As the operation or campaign progresses, the assessment plan will likely require updates to adjust to any changes in objectives, effects, and tasks. While some of these changes can be anticipated during the original assessment plan development, revisions may be necessary to reflect actual conditions in the OE or changes to the operation/campaign plan.

(3) Sometimes the assessment plan and its associated data collection may need to be refined based on changes in the IE (e.g., an information system used by the adversary is updated or replaced). This may also result in adjustments to the information or intelligence requirements to support the data collection.

(4) There should be organizational procedures associated with capturing the commander's decisions and guidance resulting from assessments that ensure necessary actions are taken. Examples include fragmentary orders, actions requiring requests for policy/authority changes or funding/resourcing requirements, additional forces needed,

partner-nation KLE requirements, other USG support from an interagency partner, or modifications to the rules of engagement.

6. Recommendations for Assessing Inform and Influence Activities

Below are some additional recommendations of particular importance for inform and influence activities:

- a. Start with objectives that are specific, measurable, achievable, relevant, and time-bound.
- b. Clearly describe the problem.
- c. Tailor assessment results to specific stakeholders, ensuring data collection, measures, and results are as transparent as possible.
- d. Throughout the assessment process, consider how commanders and other decision makers will use the assessment results.
- e. In real-world scenarios, trade-offs between precision and constraints (e.g., time, money, access) are often made to ensure assessments are conducted. It is imperative that analysts develop a plan that meets at least the minimum requirements of reliability and validity and clearly describe in detail any compromises that must be made to facilitate an assessment.

CHAPTER VII

OPERATIONS IN THE INFORMATION ENVIRONMENT

1. Overview

This chapter discusses OIE and the forces that conduct OIE. These include OIE units (i.e., those formations that JFCs may choose to assemble to conduct OIE), and information forces, which are the building blocks of those OIE units.

2. Operations in the Information Environment

a. OIE are military actions involving the integrated employment of multiple information forces to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and by protecting friendly information, information networks, and information systems.

b. OIE leverage information for the purpose of affecting the will, awareness, and understanding of adversaries and other relevant actors and denying them the ability to act in and through the IE to negatively affect the joint force, while protecting joint force will, awareness, understanding, and the ability to take actions in and through the IE.

c. OIE may provide commanders with a decisive advantage over adversaries by helping to maintain the credibility and legitimacy of joint force actions, preserving the joint force will to fight, maintaining situational understanding, and keeping the joint force free of prohibitive interference due to cyberspace or EMS activity, which cumulatively preserve freedom of action throughout the OE.

d. OIE are conducted as an integral part of all operations and campaigns and help shape the IE for future operations. As such, joint forces will always be conducting one or more OIE to remain continuously engaged in and through the IE.

e. OIE are conducted in support of all operations and may be a main effort or supporting effort.

f. Any organization or capability may be tasked to conduct activities to support OIE, whether or not assigned to an OIE unit. For example, a JTF hosting a visit by local journalists, an aviation unit conducting a show of force, or a naval strike group conducting a freedom of navigation mission may all be carrying out these activities to inform or influence relevant actors in support of OIE.

g. OIE are not a substitute for the joint forces' deliberate leveraging of the inherent informational aspects of military activities. The joint force should still integrate information and informational considerations and capabilities into strategic art and operational design, planning guidance, and planning processes.

h. OIE Limitations

(1) The ability of the joint force to conduct OIE is limited by the availability of OIE units.

(2) OIE may be limited by the capabilities and authorities of OIE units or of their higher headquarters.

(3) OIE may be more successful when integrated with other joint, Service, interorganizational, and other US and foreign mission partners.

(4) JFCs must obtain and delegate authorities to conduct specific OIE activities to be effective during crisis situations of short duration.

(5) OIE units and other information forces require prior engagement in an OE to have an understanding of, and experience in dealing with, the aspects of a problem set to be effective during crises situations.

(6) OIE require intelligence collection support during the conduct of operations to determine the effectiveness of activities.

i. OIE Mission Considerations. When planning or conducting OIE, commanders and staffs should consider:

(1) How the mission will support CCPs, the operation, campaign, OPLAN, or contingency response plan.

(2) The risks of OIE before making employment decisions. OIE may have strategic and transregional impacts beyond the employing JFC's area of operations, and commanders should consider US diplomatic and informational interests in risk calculations.

(3) Authorities and permissions required for the conduct of activities and the lead times necessary to obtain those authorities and permission.

(4) The coordination required with other joint, Service, interorganizational, and other US and foreign mission partners to align and synchronize activities and achieve unity of effort.

(5) Coordination for appropriate SME support (e.g., cultural knowledge and language skills, specialized intelligence support) and capabilities. OIE rely on joint, Service, and other mission partners for SME support.

(6) The establishment of an assessment framework during initial planning (i.e., baseline, clear MOEs, and MOE indicators).

j. **OIE Across the Competition Continuum.** Military operations vary in scope, purpose, and intensity in cooperation, adversarial competition below armed conflict, and armed conflict. Throughout the competition continuum, the JFC integrates OIE into joint plans and synchronizes it with other operations to create desired behaviors, reinforce or increase combat power, and gain advantage in the IE. Each joint operation has a unique strategic context, so the nature of OIE and its activities will vary according to the distinct aspects of the mission and OE. While OIE may be conducted as an independent operation, it is never done in isolation. OIE are conducted throughout all campaigns or operations and at any level of conflict.

For a detailed discussion of the competition continuum, including the relationship to the instruments of national power, levels of warfare, and the categories of joint military activities, see JP 1, Volume 1, Joint Warfighting, and JP 3-0, Joint Campaigns and Operations.

k. **The Joint Functions and OIE.** JP 3-0, *Joint Campaigns and Operations*, describes the seven joint functions common to joint operations: C2, information, intelligence, fires, movement and maneuver, protection, and sustainment. Each joint function is a grouping of tasks and systems that provide a critical capability to help JFCs synchronize, integrate, and direct joint operations. Commanders leverage the capabilities of multiple joint functions during operations to achieve objectives. This section presents an overview of how commanders use joint functions to integrate, synchronize, and direct OIE in support of all DOD missions.

(1) **C2 Joint Function.** C2 primarily focuses on the exercise of authority and direction by commanders over assigned and attached forces in the accomplishment of their assigned mission. That authority and direction are exercised through a C2 system that consists of the facilities, equipment, communications, staff functions and procedures, and personnel essential for planning, preparing for, monitoring, and assessing operations. The C2 systems enable the JFC to maintain communication with higher, supporting, and subordinate commands to control all aspects of current operations while planning for future operations. The C2 joint function enables the commander to balance the art of command with the science of control and integrate the other joint functions. C2 of the information planners on the staff and OIE units encompasses the exercise of authority and direction by a commander over assigned and attached information forces to accomplish the mission.

(2) **Information Joint Function.** The three tasks of the information joint function support all the other joint functions and provide commanders with the ability to understand how information impacts the OE, use information to support human and automated decision making, and leverage information through offensive and defensive actions. OIE is closely tied to the tasks of the information joint function. The understand task of the information joint function is used to understand the threats, opportunities, and vulnerabilities required to conduct OIE. It is the preparatory work that sets the stage for OIE. Additionally, the understand task should identify access points and lines of influence that can be exploited through OIE to create effects and ultimately change behavior. It also helps identify the operational signatures that need to be managed or controlled to maintain

essential secrecy. OIE uses that understanding to reveal or conceal those signatures to ensure relevant actors see what we want them to see and not see what we do not want them to see. The second task of the information joint function, support to human and automated decision making, is a critical prerequisite of effective OIE. It enables joint forces to preserve and protect our ability (and our trust in that ability) to make sense of the IE. All operations perform the third task of the information joint function, but leveraging information is the primary effort of joint OIE units.

For a more-detailed discussion on the tasks of the information joint function, see Chapter II, “Joint Force Uses of Information,” paragraph 7, “The Information Joint Function.”

(3) Intelligence Joint Function. Understanding the OE, which encompasses aspects of the IE, is fundamental to all operations to include OIE. The intelligence joint function helps to inform the JFC and staff about the opponent’s intent, capabilities, vulnerabilities, and future COAs. It also helps them to understand friendly, neutral, and threat information networks and information systems; the ways that information is received, transmitted, and processed; and how information may impact the opponent’s own decision making and drivers of their behavior. Using the continuous JIPOE analysis process, properly tailored JIPOE products can enhance understanding of the OE and clarify the impacts of information. This understanding enables the JFC to act inside the opponent’s decision cycle. JIPOE provides a socio-cultural analysis of all relevant actors to reveal their decision-making process, norms beliefs, power structures, perceptions, attitudes, and other drivers of behavior. JIPOE also reveals how relevant actors might apply information to exploit vulnerabilities in the joint force’s information networks and information systems and how they might leverage information to affect drivers of joint force behavior. Intelligence support to OIE follows the same all-source intelligence process used by all other operations, with unique attributes necessary for support of planning and assessment for OIE. The intelligence necessary to understand the drivers of behavior of enemies, adversaries, or other audiences often requires that units position and employ specific sources and methods (e.g., counterintelligence, human intelligence, targeted social media monitoring) to collect the information and conduct the analyses needed.

See Chapter IV, “Operational Design and Planning,” for a discussion of JIPOE and Chapter VI, “Assessment,” for a discussion of assessing information in joint operations.

For more details on the joint intelligence process, see JP 2-0, Joint Intelligence. For an explanation of JIPOE, see the Joint Guide for Joint Intelligence Preparation of the Operational Environment.

(4) Fires Joint Function. Fires is the use of weapon systems or other actions to create specific lethal or nonlethal effects on a target. The nature of the target or threat, the conditions of the mission variables (i.e., mission, enemy, terrain and weather, troops and support available, time available, and civil considerations), and desired outcomes determine how lethal and nonlethal capabilities are employed. OIE may leverage the inherent informational aspects of joint fires. Fires in and through the IE encompass a

number of tasks, actions, and processes, including targeting, coordination, deconfliction, and assessment (e.g., BDA).

(a) OIE tasks and capabilities leverage information through fires to create specific effects. To integrate effectively, information planners participate in the joint targeting process by selecting and prioritizing targets for fires or TAs for other actions. OIE units create fires that typically result in nonlethal effects. OIE can also indirectly create effects that result in physical destruction (e.g., manipulating computers that control physical processes). Additionally, OIE can leverage the inherent informational aspects of fires to reinforce the psychological effect of those fires. OIE may rely on joint fires support to transmit information to relevant actors and to deliver nonlethal payloads to affect information, information systems, and information networks (e.g., leveraging CO to deliver computer code designed to deny network access to an adversary, PA releases to inform friendly audiences, or MISO products to influence foreign audiences).

(b) The integration of OIE into the targeting process—a task managed within the fires function—is important to creating effects in and through the IE that will achieve objectives. Even when OIE do not require joint fire support to create effects, they still depend upon the joint targeting process to integrate and deconflict fires effects that may impact strategic- and operational-level objectives (see Chapter IV, “Operational Design and Planning,” paragraph 4.b.(3)(c), “Select and prioritize audiences, TAs, and targets”). It is important to note that not all forms of information fires dovetail into the targeting process; in some instances, these fires bypass the targeting process to go directly to the effects board. For instance, if the JFC’s intent is to influence a relevant actor to participate in peace negotiations during armed conflict, all participants in the targeting process must ensure lethal fires and joint force combat actions do not inhibit or dissuade that participation. Information planners participate in the targeting process as members of the joint targeting coordination board, which plans, coordinates, and deconflicts joint targeting.

(c) Like all forms of fires, fires in support of OIE are included in the joint planning and execution processes to facilitate synchronization and unity of effort. JFCs use coordination and control measures to enable joint action. These measures include strategic and operational mission narratives, PAG, other communication-related guidance, the law of war, and rules of engagement. Additionally, information planners identify control measures for OIE that have the potential to conflict with the OIE of other CCMDs or interorganizational partners. OIE units work with maneuver and fires elements to establish fire control measures to reduce the impact of combat operations on the civilian populace. If multiple USG or allied entities have requirements to create effects or collect intelligence on the same target in the IE, then synchronization and deconfliction across all USG entities are critical to prevent uncoordinated actions from exposing or interfering with each other.

(d) Finally, units conducting OIE contribute to, and benefit from, the joint fires task of assessing the results of employing fires. That task includes assessing the effectiveness and performance of fires, as well as their contribution to the larger operation or objective.

For details on joint targeting, see JP 3-60, Joint Targeting.

(5) Movement and Maneuver Joint Function

(a) Maneuver is the employment of forces in the JOA through movement in combination with the other joint functions to gain a position of advantage in respect to the enemy. The movement and maneuver joint function encompasses the disposition of joint forces to conduct operations by securing advantage and exploiting tactical success to achieve operational and strategic objectives. Movement and maneuver to and within the JOA can signal adversaries, allies, and neutral actors and may have a deterrent or assuring effect in support of JFC objectives. Movement and maneuver involve deploying forces and capabilities into a JOA and positioning them within that area to gain operational advantage in support of mission objectives, including accessing and, as necessary, controlling key terrain. Movement and maneuver of forces have inherent informational aspects that affect the achievement of JFC objectives and should be accounted for during planning and execution.

(b) OIE, the art of maneuvering in the IE, is conducted to enhance the effects of the inherent informational aspects of the movement and maneuver of forces. The pervasive nature of information and the IE provides the joint force with operationally significant access to relevant actors within the JOA, as well as outside the JOA. OIE contribute to the joint force's freedom of action and control of the operational tempo necessary to conduct its activities at a time and place of its choosing to produce the operational reach necessary to create an advantage over the adversary.

For more information on maneuvering in cyberspace, see JP 3-12, Joint Cyberspace Operations.

See JP 3-85, Joint Electromagnetic Spectrum Operations, for a discussion of maneuvering in the EMS.

(6) Protection Joint Function. The protection joint function provides the JFC with the capabilities needed to protect the joint force, its bases, necessary infrastructure, and lines of communication from attack. The protection joint function complements the information joint function by ensuring the use of appropriate physical defensive measures necessary to safeguard information. With respect to OIE, the protection joint function attends to the physical security necessary for the deployment, storage, employment, and redeployment of SAP capabilities necessary for classified OIE. As part of OIE, DODIN and DCO secure and defend the joint force's information, information networks, and information systems that form the backbone of the JFC's C2 joint function. Due to their global and commercial connectivity, protection of these assets is complicated. OIE reinforces the protection function by degrading the opponent's ability to target the joint force by attacking its information, information networks, information systems, and human and automated decision making. For example, OIE that include OCO and JEMSO (e.g., jamming communication frequencies) can protect the joint force by disrupting the

opponent's targeting and C2 systems. OPSEC also supports the protection joint function by protecting critical information.

(7) **Sustainment Joint Function.** The sustainment joint function provides the JFC with the capabilities necessary to provide the logistics and personnel services required to maintain and prolong joint operations until mission objectives are achieved. Successful execution of OIE requires that information be regarded as a mission-essential resource that must be sustained (e.g., assuring its integrity, accuracy, confidentiality, accessibility, nonrepudiation, and flow). Joint operations, especially globally integrated operations in the IE, may require those portions of the joint force that conduct OIE to be geographically dispersed and virtually connected, which will require special considerations for sustainment. Sustainment support for the OIE unit is essential and requires coordination with the joint force's logistics staff. Sustainment contributes to the joint force's ability to generate effects and operate in the IE. From an operational perspective, OIE can help protect sustainment efforts by manipulating or masking the inherent informational aspects of joint force sustainment activities in ways that impair an opponent's ability to sense and target these efforts.

For a discussion of joint functions, see JP 3-0, Joint Campaigns and Operations. The protection of the DODIN is discussed in JP 3-12, Joint Cyberspace Operations, and JP 6-0, The Joint Communications System. See JP 13-13.3, Operations Security, for more details on OPSEC.

3. Organizing for Operations in the Information Environment

a. JFCs may choose to create a task force for the integrated employment of the specialized capabilities required to conduct OIE.

b. Information forces, the building blocks of OIE units, are those Active Component and Reserve Component forces specifically organized, trained, and equipped to create and/or support the creation of effects on the IE. Information forces aggregate military personnel, weapon systems, equipment, and necessary support that provide expertise and specialized capabilities (e.g., CMO, MISO, PA, EMSO, CO) that leverage information and conduct activities central to OIE. See paragraph d., "Information Forces," below, for a discussion of the types of information forces that make up OIE units.

c. **Organizations and Personnel.** OIE units consist of a headquarters organization with C2 of assigned and attached information forces.

(1) OIE unit personnel include information planners and support personnel (e.g., intelligence, logistics). Information professionals are information force personnel who are specifically trained to inform audiences; influence external relevant actors; attack and exploit relevant actor information, information networks, and information systems; and protect friendly information, information networks, and information systems. Information planners serve in OIE units and as OIE and specialized capability SMEs on JTF and other headquarters planning staffs.

(2) OIE unit headquarters are composed of a commander and a staff of information planners who possess a depth of knowledge and experience in their respective fields, as well as broad experience working alongside planners from other fields.

d. **Information Forces.** OIE units are typically composed of the following types of information forces:

(1) **Psychological Operations Forces.** Psychological operations forces consist of personnel trained and equipped to conduct MISO. MISO are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the JFC's objectives.

For additional guidance on psychological operations forces and MISO, refer to JP 3-13.2, Military Information Support Operations.

(2) **CA.** CA are actions planned, coordinated, executed, and assessed through civil reconnaissance, network analysis, and network engagement to support, influence, compel, or leverage populations, governments, and other institutions to expose malign influence, counter coercion and subversion, and impose costs through conventional and unconventional activities. CA forces execute CA operations and enable the commander's CMO, engaging the civil component of the OE to support the JFC's CMO efforts. CA enhance awareness of and manage the interaction with the civil component of the OE, identify and mitigate underlying causes of instability within civil society, engage and influence civil networks, and support other information activities.

For additional guidance on CA and CMO, refer to JP 3-57, Civil-Military Operations.

(3) **PA Organizations.** PA organizations and personnel focus on the OIE core activity of informing domestic, international, and internal audiences. They contribute to the achievement of OIE objectives by putting joint operations, activities, and policies in context; facilitating informed perceptions about military operations; countering disinformation and propaganda; and correcting misinformation through the dissemination of timely and accurate information. PA personnel participate in staff planning and lead the collaborative development of operational- and tactical-level narrative development. They contribute to the development of constraints and restraints, the identification of potential intended and unintended consequences of planned actions, and to an appreciation of the nature of information flow in varying cultural contexts. PA planners advise the JFC on the possible direct and indirect effects of joint force actions on public perceptions, attitudes, and beliefs and work to formulate and deliver timely and culturally attuned messages.

For additional guidance on PA, refer to JP 3-61, Public Affairs.

(4) **EMSO Elements.** EMSO elements assigned to OIE units work with the JEMSO at the parent command to organize, execute, and oversee the conduct of EW and

spectrum management. They do this as part of OIE and, when tasked, in support of other joint force operations. Because EMSO is an enabler for other activities that communicate through or use the EMS, such as MISO, PA, or CO, EMSO elements work closely with information planners from other fields on the OIE unit staff.

For additional guidance on EMSO, refer to JP 3-85, Joint Electromagnetic Spectrum Operations.

(5) **Cyberspace Forces.** Units of the CMF include cyberspace protection teams that defend blue cyberspace in reinforcement to the system operators and local defenders; national mission teams, supported by national support teams, that defend the nation from threats in cyberspace by operating in gray and red cyberspace; and combat mission teams, supported by combat support teams, that project power in support of CCDR objectives, by operating in and through gray and red cyberspace. Units of the cyberspace forces retained by the Services or assigned to the CCMDs conduct similar missions of more limited scope. Mission-tailored force packages of cyberspace forces and cyberspace capabilities are established as required and can include small mission elements selected from one or more teams up to named JTFs.

For additional guidance on cyberspace forces, refer to JP 3-12, Joint Cyberspace Operations.

(6) **Space Operations Elements.** USSF Guardians assigned as planners on OIE unit staffs ensure commanders and their staffs have a common understanding of space operations, provide space domain awareness, and coordinate space capabilities for OIE. Space operations support the flow and protection of information and decision making and are an enabler for other activities that communicate through or use space capabilities.

For additional guidance on space operations, refer to JP 3-14, Joint Space Operations.

e. OIE Unit Core Activities

(1) **Introduction.** OIE unit core activities include conducting OIE and facilitating the JFC's integration of information into joint force operations.

(a) These core activities reflect the collective abilities of OIE units rather than those of any one Service or unit. OIE unit core activities are organized into missions that contribute to achieving a commander's objectives. OIE units may conduct one or both core activities during the conduct of a mission.

(b) Other joint force elements conduct some of the information activities associated with these core activities during their operations. However, OIE units conduct these core activities with assigned capabilities in a manner that complements and supports joint force abilities to achieve a broad range of strategic and operational objectives. For example, a ground maneuver element might conduct a MILDEC activity in support of its own mission to get an enemy decision maker to move forces to a location where they could

be destroyed, but a JFC would task an OIE unit to conduct MILDEC as part of OIE that is focused more broadly on the JFC's objectives. Likewise, all of the joint force's subordinate elements have a responsibility to understand how information affects their OE, but the OIE unit conducts that activity at the direction of and for the JFC.

(2) **OIE.** OIE are the primary focus of OIE units. OIE encompass critical tasks that OIE units must perform to achieve JFC objectives by leveraging information. OIE units accomplish these tasks using military capabilities in a coordinated and synchronized manner to collectively achieve objectives affecting the IE by informing audiences; influencing foreign relevant actors; attacking and exploiting information, information networks, and information systems; and by protecting friendly information, information networks, and information systems. OIE are conducted in support of the JFC's operation or campaign objectives or in support of other components of the joint force. Joint forces continuously conduct OIE to remain engaged with relevant actors.

(a) The inform task involves actions taken to accurately communicate with domestic and foreign audiences to build understanding and support for operational and institutional objectives. It seeks to reassure allies and partners and to deter and dissuade competitors, adversaries, and enemies. The inform task uses accurate and timely information and visual media to counter disinformation; correct misinformation; and put operations, activities, and policies in context. It involves communication with domestic and international audiences and with joint force personnel. Planning and executing tasks to inform include public engagement and the acquisition, production, and dissemination of communication and other information products. The inform task facilitates educated perceptions by establishing facts and placing joint force activities in context, correcting inaccuracies and misinformation, and discrediting propaganda with counter-narratives. The primary means used for the inform task is PA; however, CA, cyberspace, and psychological operations forces can facilitate the release of truthful information through their respective CMO, CO, and MISO activities.

(b) The purpose of the influence task is to affect the perceptions, attitudes, and other drivers of relevant actor behavior. This task is focused on impacting the human aspects of the OE, so planners should consider elements of these aspects as they relate to decision makers (e.g., each decision maker's culture, life experiences, relationships, outside events, ideology, and the influences of those people inside and outside the decision maker's group) during OIE planning, execution, and assessment. Planners integrate influence activities into the existing targeting process. Activities designed to contribute to the influence task include MISO, CMO, CO, OPSEC, and MILDEC operations. Influence may also involve the use of STO. Commanders consider the influence potential of all available capabilities in design, planning, and targeting. OIE units conduct all influence tasks in accordance with approved authorities.

(c) The attack and exploit task comprises activities meant to impact or use opponent information, information systems, and information networks in ways that affect decision making and other drivers of behavior to create relative advantages for the joint force. OIE units execute these actions to manipulate or paralyze the adversary or enemy

decision-making processes. Attack activities encompass affecting the real or perceived accuracy, integrity, authenticity, or confidentiality of information or the availability of information. OIE units accomplish attack tasks through technical means, such as CO, EMSO, and STO, though maneuver forces and joint fires can also be employed in support of these tasks. Exploit activities include accessing information, information networks, or information systems to gain intelligence and support operational preparation of the environment (OPE) for current or future operations. OPE may subsequently support inform and influence tasks of OIE. OIE units accomplish the exploit task through technical means, such as CO or EMSO.

(3) Facilitate the JFC's integration of information into joint force operations.

(a) OIE units have the responsibility of supporting the JFC's integration of information into the planning and execution of all joint force operations and activities. This encompasses maintaining an understanding for the JFC of how information affects their OE; providing advice and assistance on how to best leverage the inherent information aspects of all joint force activities; collaborating with the JFC staff on the protection of information, information networks, and information systems; and assessing the effectiveness of joint force activities from an informational perspective.

(b) OIE units accomplish this with assigned, attached, or supporting intelligence capabilities and analysts in conjunction with the joint force intelligence staff. It includes providing analysis of the informational, physical, and human aspects of the environment; identifying threats, vulnerabilities, and opportunities in the IE; and identifying and analyzing relevant actors.

See Chapter II, "Joint Force Uses of Information," paragraph 7, "The Information Joint Function," for details on the task understand how information impacts the OE.

(c) OIE units conduct this core activity by providing original products to the staff (e.g., analysis of the informational, physical, and human aspects of the environment), input to staff products (e.g., military narrative, information estimate), or participating in the JPP with the staff. OIE units do this via planners serving on, or as liaisons to, higher headquarters staffs or through coordination between their staff and higher headquarters staff.

4. Operations in the Information Environment: Planning, Coordination, Execution, and Assessment

a. JPP and OIE

(1) Commanders integrate OIE into their operations at all levels. Plans should address how OIE affect the will, awareness, and understanding of adversaries and other relevant actors; deny competitors the ability to act in and through the IE to undermine the

joint force; and protect joint force will, awareness, understanding, and the joint force ability to take actions in and through the IE.

(2) JFCs integrate OIE into operations, as main or supporting efforts, or conduct an OIE as a stand-alone effort. During plan development, JFC provides planning guidance that describes the desired conditions that must exist in the IE to support mission accomplishment, how the joint force will leverage the inherent informational aspects of its activities to support the JFC's objectives, and the types and level risk that the JFC will accept in the IE. Specifically, for OIE units, the JFC provides guidance on how OIE will support the JFC's scheme of maneuver. The JFC ensures supporting OIE plans and concepts describe the role and scope of OIE in the JFC's effort and address how OIE support the execution of the JTF plan.

(3) OIE are planned using the JPP. Planners integrate OIE unit capabilities into the JPP as a part of adaptive planning.

b. OIE Planning Considerations

(1) **Overview.** Information planners have the same operational design considerations and challenges as planners for operations in the physical domains but also have some unique considerations for planning OIE. While OIE plans are developed to inform and influence, and to affect or protect information, information networks, and information systems, but there are factors outside the control of OIE that will have impacts in and through the IE that undermine those plans. These factors range from unanticipated adversary or mission partner actions inside the JOA to natural disasters or unforeseen domestic social or political developments that occur outside of the JOA that, nonetheless, affect the JFC's OE. Regardless of the event or action, they create conditions to which OIE planners must adapt and have the flexibility to address in branch plans or sequels.

(2) **Different Planning Considerations for Contributing Information Forces.** Each of the information forces that contribute to OIE (e.g., psychological operations forces, cyberspace forces) has their own unique planning considerations that increase the complexity of planning OIE. For each capability or activity employed, OIE planners will need to understand the different authorities and permissions, coordination requirements, intelligence requirements, and account for the lead time necessary to satisfy these requirements prior to the execution of activities.

(3) **Planning and Execution Timelines.** Related to the above, the applicable authorities will vary depending upon when and where the activities occur and what or whom they will affect (e.g., if effects are likely to impact other relevant actors outside of a JFC's operational area). This includes accounting for the lead time required to obtain the necessary intelligence for target development and target access; confirm the appropriate authorities; and complete necessary coordination, including interagency coordination and/or synchronization. Additionally, planners will need to understand the length of time it will take for certain actions to have the desired effects and the duration of those effects.

This may require OIE to begin prior to other joint force activities or even continue after some of those activities cease.

(4) **Language, Regional, Cultural, or Technical Expertise.** Leveraging information for the purpose of affecting the behavior of relevant actors requires an understanding of the drivers of human or automated systems behavior. These drivers include language, regional, cultural, and often technical aspects. Planning teams will need to obtain support from various SMEs with an understanding of these aspects to understand relevant actors and develop feasible plans.

(5) **Plan for Monitoring Effects and Adjusting Activities.** The dynamic nature of the IE often makes it challenging to determine whether OIE are effective. Planners of OIE should determine MOEs and MOE indicators during initial planning, incorporate monitoring tasks as essential elements of all OIE plans, and obtain adequate support to fulfill information and intelligence requirements.

(6) **Unintended Effects in and through the IE.** The inherent informational aspects of activities and the lack of boundaries in the IE guarantee that military activities will often have impacts in and through the IE beyond the intended area or relevant actor. This makes the evaluation of potential effects particularly important when conducting OIE. Information activities can cause effects in and through the IE in ways that are not evident to planners. Some of these effects may affect other commanders' areas of operations and objectives or have strategic impacts. Coordinating plans and activities with joint, USG, and other mission partners will help identify potential effects beyond those intended and allow planners to avoid or mitigate effects that jeopardize their own or mission partner objectives.

c. **Intelligence Support to OIE.** The complexity of OIE requires dedicated intelligence support. Intelligence professionals will need to work closely with OIE planners throughout the planning, execution, and assessment of operations to ensure they understand and meet the unique OIE information and intelligence requirements.

(1) **Intelligence requirements.** During OIE mission analysis, the planners identify significant information gaps about the adversary and other relevant aspects of the OE. After gap analysis, the staff formulates intelligence requirements, which are general or specific subjects upon which there is a need for the collection of information or the production of intelligence. Based upon identified intelligence requirements, the staff develops more specific questions known as information requirements (those items of information that must be collected and processed to develop the intelligence required by the commander). Information requirements related to the IE will include questions about the informational, physical, and human aspects of the environment; the questions about the characteristics of relevant actors; and the impact of the aspects of the environment on relevant actor behavior. These intelligence requirements are fulfilled through a combination of military intelligence and national intelligence sources.

See JP 2-0, Joint Intelligence, for additional details on intelligence requirements.

(2) **RFIs.** Planners can submit RFIs to obtain intelligence products that support their activities or trigger collection efforts in any part of the OE. RFIs are specific, time-sensitive, ad hoc requirements for intelligence information to support an ongoing crisis or operation and not necessarily related to standing requirements or scheduled intelligence production. RFIs fulfill customer requirements and range from disseminating existing products through integrating or tailoring on-hand information to scheduling new collection and production. RFI managers work closely with the OIE planners to understand the OIE information requirements and translate those requirements into RFIs. The RFI manager and the primary intelligence producer determine how best to meet those requirements. In addition to information collected during military operations, information required to support OIE planning can come from signals intelligence, human intelligence, counterintelligence, measurement and signature intelligence, geospatial intelligence, or open-source intelligence. Regardless of source, the information should be timely, accurate, and in a usable format.

See JP 2-0, Joint Intelligence, for additional information on RFIs.

d. **Targeting.** Commanders may choose to engage relevant actors through lethal and/or nonlethal fires as part of OIE. Relevant actors selected for engagement through joint fires are developed, vetted, and validated within the established targeting process. Planning and targeting staffs develop and select relevant actors for targeting in and through the IE based on the commander's objectives rather than on the capabilities available to achieve them. The focus is on creating effects that accomplish targeting-related tasks and achieve objectives, not on using a particular capability simply because it is available. For a discussion of relevant actors and targeting, refer to Chapter IV, "Operational Design and Planning," paragraph 4.b.(3)(c), "Select and prioritize audiences, TAs, and targets."

For details on joint targeting see JP 3-60, Joint Targeting.

e. C2 of OIE Units

(1) The complex and dynamic nature of the IE, where all joint force activities cause effects in and through that environment, make unity of effort crucial for all effective operations, including OIE. The JFC promotes unity of effort through the integration of information considerations into the planning and execution of all joint force operations, as discussed in Chapter IV, "Operational Design and Planning." The JFC may reinforce this unity of effort with unity of command by establishing a subordinate task force so the preponderance of information forces' capabilities and activities are the responsibility of one commander under the JFC.

(2) The JFC provides OIE unit commanders with the authorities, processes, and tools required to C2 assigned and attached units. The JFC will also provide OIE unit commanders the appropriate level of control of additional forces necessary to accomplish OIE missions.

(3) The JFC assigns OIE units missions to create effects in and through the IE to set conditions that support the JFC's objectives and enduring outcomes.

f. Synchronization of OIE Activities

(1) By its nature, OIE involves the synchronization of multiple capabilities and activities to aggregate their effects and achieve operational objectives. Synchronization comprises the coordination, tracking, and direction of all OIE activities to ensure they are aligned with the JFC's overarching narrative and objectives, and synchronized and deconflicted with activities external to the command.

(2) An OIE unit achieves internal synchronization through a commander-led joint planning and execution processes for all OIE. This includes planning the conduct of information activities by assigned and attached information forces to create effects in the IE resulting in the publication of a synchronization matrix during orders generation. Through and following orders generation, OIE units position and employ their elements in accordance with the synchronization matrix to create desired effects at the right time and place.

(3) Due to the interconnectedness of the IE, the effects of activities in and through the IE may cross geographical boundaries and, if not carefully planned and synchronized, may have unanticipated effects on tactical up through strategic-level objectives. OIE should be coordinated with other DOD entities, the interagency, and multinational partners so objectives and activities are deconflicted and, to the greatest extent possible, synchronized to create greater effects. Coordination of OIE with external organizations is through information planners or other personnel serving on higher headquarters staff or at adjacent joint and mission partner units. Coordination is accomplished with multinational partners via the staff unless otherwise authorized.

For details on interorganizational collaboration, see Chapter III, "Unity of Effort."

g. Assessment of OIE Activities

(1) Assessment helps the commander determine progress toward achieving joint force objectives and mission accomplishment. This requires identifying current (baseline) conditions of the OE and determining those desired conditions that define achievement of objectives, then monitoring for change from the current to desired conditions. Measuring this progress toward the mission objectives and delivering feedback into the planning process to adjust operations during execution involves deliberately comparing the planned effects of OIE with actual outcomes to determine the overall effectiveness of OIE unit activities.

(2) The assessment process for OIE begins during planning and includes developing MOEs and MOPs of OIE activities, as well as their contribution to the larger operation or objective. This includes identifying MOE indicators and incorporating monitoring tasks as essential elements of those OIE plans. Historically, combat assessment

has emphasized the BDA component of measuring physical and functional damage, but this approach does not always represent the most complete effect, particularly with respect to OIE. OIE often seeks to have effects outside the scope of battle and often do not create physical damage. While assessing the effects of OIE may require typical BDA analysis and assessment of physical, functional, and target system components, the higher-order effects of actions in and through the IE are often subtle. Assessment of second- and third-order effects of OIE activities can be difficult and may require significant intelligence collection and analysis efforts. Clearly articulating the desired effects and creating and resourcing an assessment plan for OIE during the planning processes increases the likelihood that all objectives are met. Planners should emphasize JIPOE, COG analysis, target systems analysis, and collection management activities to inform assessment.

For details on assessment of information activities, including OIE, refer to Chapter VI, "Assessment."

APPENDIX A

NARRATIVE DEVELOPMENT

“There is empirical evidence that experiencing a narrative can be transformational and can induce long-term effects upon audiences’ beliefs, attitudes, and behavioral intentions and actions.”

Brigadier General Tim Fay and Dr. Jorge Barraza, *Leveraging Neuroscientific and Neurotechnological Developments with Focus on Influence and Deterrence in a Networked World*

1. Principles of Developing Narratives

Successful military operations depend on creating an operational advantage in a highly complex and dynamic IE. To meet this challenge, the joint force communicates the rationale for their actions to a wide range of friendly, neutral, and adversarial audiences. This need to communicate a rationale is just as true for military operations conducted in a poorly developed area that depends on word-of-mouth to remain informed as it is for operations conducted in a highly technologically connected environments inundated with sources of information. If planners fail to provide a narrative that provides an observer with context for sense-making, observers will use their own narratives to explain the military events around them, which may or may not advance the commander’s overall intent. Developing an effective narrative helps audiences from the individual military member to international audiences understand the reasons behind joint force activities. This appendix describes a seven-step process for developing a narrative.

2. Characteristics of an Effective Narrative

Applied narrative research has demonstrated that effective narratives can and do affect rationality, decision making, and other aspects of thought processes. A narrative focused on meaning is more effective and more persuasive than a narrative that relies on one-way communication strategies that focus on transmission of messages. Studies have shown that an effective narrative:

- a. Provides coherence to military actions and activities through a structured expression of the reasons for and the desired outcomes of the campaign/operation.
- b. Is easily understood and remembered by intended audiences.
- c. Describes the context of the organization (e.g., JTF, CCMD), why it does what it does, and ideally something about what it does.
- d. Makes clear and removes the ambiguity of US values and interests regarding the current situation.

e. Provides a more compelling and believable alternative for the future than the outcomes the adversary is attempting to portray. Ideally, it does so by exploiting adversary weaknesses and mitigating adversary strengths.

f. Offers a better and just future regarding the contested interest. This future should appeal to emotions and demonstrate an awareness of the audiences' values and social norms.

g. Is logical, meaning it falls within the belief system of the intended audience (e.g., linguistically, culturally, socially). Presenting a logical narrative is not about including a bunch of facts. It is about presenting a narrative that is grounded in the realities of the situation, including important factors within PMESII systems.

h. Supports the development of a common identity (e.g., shared values, goals) and a desired image of the force that is necessary to integrate words and deeds and thus creating desired effects in the IE.

i. Is easily communicated through credible sources. This means it should be unclassified and written so that it can be shared with partners and publics without jeopardizing the mission.

3. Narrative Hierarchy

a. As part of campaigning, the joint force helps develop and employ military strategic and cascading mission narratives that reflect policy aims and are targeted at the adversary. The President or national security staff may provide a strategic narrative that includes national-level communication guidance. More often, the national-level strategic narrative will have to be derived (understood) from guidance (e.g., NDS, NSC talking points, speeches). DOD, either the JS or OSD, then develops a military strategic narrative that explains the use of the military and puts global operations in context.

b. CCMD and operational-level headquarters staffs develop cascading operational-level mission narratives with their associated themes and messages that nest under the strategic military narrative. These operational-level narratives focus on the theater/region and seek to advance the legitimacy of the mission while countering adversary narratives. Staffs at this level should assess whether the narrative audience operates on a global stage, exposing them to narratives of other JFCs. If so, planners should ensure narrative synchronization with other narratives to minimize potential blue-on-blue narrative confliction and strive to maximize TA narrative engagement. This will enhance narrative penetration and reduce “say-do gap” possibilities. The joint force should make every effort to ensure operations, activities, words, and images are perceived as being consistent with this narrative.

c. Tactical units develop a local tactical mission narrative nested under the operational mission narrative to lend continuity to operations and communications. Figure IV-2 in Chapter IV, “Operational Design and Planning,” shows how these narratives flow from the

national level through the operational to the tactical. Component and tactical force narratives for audiences operating on the global stage should be deconflicted and synchronized with component and tactical forces with the potential to convey the narrative. This collaboration is critical to minimize “say-do gaps” and ensure narrative coherency and consistency.

d. In addition, commanders ensure the mission narrative is communicated internally to their forces. Communicating the narrative internally helps forces understand the necessary conditions and their roles in achieving the objectives. Internal and external harmonization of narrative efforts is paramount for the development of both a common identity and a desired image of the command/unit. Communicating a clear and compelling narrative internally fosters a sense of common purpose and shared direction. Internal communication of the narrative enables military personnel to better understand their roles by explaining the legitimacy of policies, programs, and operations affecting them. This understanding helps protect forces against malign influence.

4. Developing the Narrative

Narratives are developed through a PA-led collaborative effort that reflects what the mission itself is likely to communicate or signal to those audiences observing it. Primary collaborators for narrative development are PA, psychological operations forces, J-5 KLE personnel, the POLAD and staff, and intelligence planners.

a. **Incorporate Guidance/Strategic Narrative.** Strategic guidance initiates planning, provides the basis for mission analysis, and enables the JPEC to develop a shared understanding of the issues, OE, objectives, and responsibilities. A strategic narrative is constructed for the purpose of providing common guidance for subordinate forces to communicate that shared understanding effectively and accurately. As mentioned, the strategic national narrative with national-level communication guidance may be provided by the President or national security staff. More often, planners will need to derive the national-level narrative from strategic guidance such as the NSS, NMS, NSC talking points, and speeches. Commanders’ guidance informs development of the military mission narrative by providing the purpose, aim, and scope of the mission. Mission analysis supports development of the narrative by providing an understanding of the overall situation and its root causes. A key output from mission analysis is the identification of the actors that are most relevant to the campaign or operation.

b. **Narrative Analysis.** Narrative analysis is used to gain greater understanding of the OE. Narratives are always in existence, whether we purposefully create them or not. They exist because every culture transmits and sustains its own narratives that provide it with its own identity and basis for actions. Before crafting their own narrative, joint force planners need to understand what narratives exist in the OE, what they reveal about relevant actors, and how they are propagated.

(1) **Narrative landscape.** The joint force will face pre-existing, and potentially competing, narratives. Understanding this narrative landscape helps the joint force to

predict how audiences will receive and interpret information. Prior to developing the narrative, the joint force should identify what narratives exist in the OE, which ones are prevalent, and which ones seem to be most effective.

(2) **Narrative content and form.** Narratives can provide information from relevant actors' cultural perspective about what they consider important, how they interpret events, and how they are being positively or negatively impacted. Narrative content includes the story or message that is communicated, the symbols used, the actors involved, and the meaning of the message for the narrator. Narrative form includes the structure of the narrative, the sequencing of events, and how language is used. Information professionals, regional-cultural experts, and other SMEs can help analyze the content and form of existing narratives.

(3) **Narrative transmission.** How the various narratives are disseminated, received, and processed not only helps identify effective communication paths but can also reveal key influencers in the IE. Understanding how relevant actors communicate and exchange information will impact how the joint force will craft and communicate its narrative. The primary executors of the mission narrative are personnel who routinely interact with the local populace.

c. Audience Analysis

(1) An audience is a broad, roughly defined group based on common characteristics. It defines a group or population to whom the military intends to communicate. Audiences can include the US populace, regional parties, allies, NGOs, international organizations, private sector, foreign populations, and adversaries. Each audience views words, images, and deeds through their cultural lens and local environmental conditions. Each uses trusted communication mediums to receive, process, and disseminate information. Audience analysis informs the joint force's planning to inform and influence key audiences, recognizing the responsibility to provide factual information, particularly to US and friendly audiences.

(2) Commanders and staff attempt to understand the many audiences within the operational area, across the broader region, and around the world to develop a compelling narrative and deliver messages using the appropriate means to educate, inform, and influence those audiences. Each audience has its own beliefs and perspectives, which affect how it perceives our actions and words, often in ways we may not anticipate. Each audience receives information differently—whether by word of mouth, written texts, Internet (including social media), radio, or television.

(3) Intelligence, PA, CA, and MISO staff all perform some type of audience analysis. Intelligence staff use socio-cultural analysis and a system perspective to identify and analyze all relevant actors, to include their relationships and interdependencies (see JP 2-0, *Joint Intelligence*). PA officers use quantitative and qualitative research to better understand internal and external publics, and the cultural landscape to better understand audience needs and predispositions, and better design messages to increase audience

understanding (see JP 3-61, *Public Affairs*). CA professionals understand the key audiences within the civil dimension by analyzing the six interrelated civil considerations: areas, structures, capabilities, organizations, people, and events (see JP 3-57, *Civil-Military Operations*). MISO planners follow a MISO-unique TAA model to analyze potential or approved foreign TAs' current attitudes and behavior, their ability to accomplish desired behavior change, their accessibility by various dissemination means, and their susceptibility to influence. TAA includes a thorough examination of the political, military, economic, cultural, religious, psychological, environmental, physical, and social conditions that shape the OE and influence the behavior of the individuals and groups (see JP 3-13.2, *Military Information Support Operations*). Common questions that can be answered by audience analysis are:

- (a) Who are the various audiences, their beliefs, and relationships to others?
- (b) Who are the friendly audiences that we need to inform and what is the best way to inform them?
- (c) Who are the neutral audiences that might potentially support friendly objectives or the adversary, and how may they be engaged?
- (d) Who are the adversary's supporters or potential supporters and how can they be influenced?
- (e) What are the audience's rules, customs, norms, beliefs, and motivations?
- (f) What linkages and relationships exist within the audience that can be leveraged?
- (g) What are the trusted mediums (conduits) through which the audience receives information (governmental, academic, cultural, and private enterprise) and by what means (Internet/social media, radio, face-to-face, television)?
- (h) How can effects be observed/measured (informs assessment which is addressed below)?
- (i) In addition to the TA, which audiences might also receive the narrative and how would they perceive and react to it?

d. **Audience Accessibility.** Planners consider the various ways in which narratives may be conveyed to audiences. Considerations for reinforcing the narrative are:

- (1) What are the means that can be used to provide multiple/reinforcing communication channels?
- (2) What capabilities (physical or informational) are available for this operation?

- (3) What methods of communication will be effective in reaching audiences?
- (4) How does the joint force identify the right conduits and then access those conduits?
- (5) What are the audiences' critical networks (formal and informal)?
- (6) How does the joint force identify and analyze potential communication media and channels?
- (7) How does the joint force identify relevant actors' physical communication and human networks?

e. **Writing The Narrative Statement or Paragraph.** A narrative can be detailed and complex with lots of background details. These details from the narrative development process should be documented for later use by information professionals. This detailed narrative should be expressed in plans and orders through a concise statement or paragraph that articulates the conditions, opportunities, key actions, and payoffs associated with a particular mission/operation/campaign. The first three steps of narrative development make it possible to construct a concise but comprehensive written narrative statement, which can stand on its own and support the creation of local narratives that will resonate with specific TAs. It is important that this written narrative statement or paragraph conveys the commander's reasons and desired outcomes for the campaign/mission/operation.

- (1) **Elements of a narrative.** There are four elements to the written narrative:

- (a) **The current state.** This includes a description of the current problem and why it is important. This can be a wrong that will be righted or a desirable condition to be retained. Additional details can describe what has been done up to now and what will happen if nothing is done.

- (b) **The desired future state.** This includes a description of the necessary behaviors and conditions required to accomplish the mission. It should describe what good or right looks like in terms that the audience can understand.

- (c) **The pathway.** This includes a description of how the joint force intends to get to the desired future state. It answers the questions of what will be done, who it will be done to, and who it will be done with.

- (d) **The justification.** This includes a description of why the proposed future state is better than the alternatives, thus validating the pathway. The justification is best when woven into the other three elements.

- (2) **Narrative Storytelling.** The narrative statement/paragraph provides a framework for communicating meaning that goes beyond simple transmission of messages and themes. In crafting the narrative, writers should consider components/elements of

storytelling. These components are characters, traits, goals, motives, conflict and problems, risk and danger, struggles, and details. These components are conveyed through words, deeds, and images. Carefully crafting a narrative with these components of storytelling increases the likelihood that the audience will make sense of the narrative. Storytelling can create an emotionally appealing narrative that elicits personal investment in the audience.

(3) **Themes and Messages.** A narrative provides a cohesive background story for themes and messages. If the themes, messages, operations, and imagery (also known as words, deeds, and images) are not synchronized, contradictions may emerge and can be exploited by the enemy. Themes are distinct, unifying ideas or intentions that support the narrative. These narratives and themes enable the development of discrete messages and ideas relevant to specific audiences and are delivered through words, actions, and images. Messages support themes by delivering tailored information to the specific public for delivery at a specific time, place, and communication method. While messages are more dynamic, they must always support the more enduring themes up and down the chain of command. Messages should support the themes at their specific level. The themes should support (or be nested under) the next higher-level themes and support the overarching narrative.

f. **Approval and Placement in Plan/Order.** It is essential that narratives are approved and endorsed by the commander to achieve permanence. The approval process should allow for multiple reviews, but pretesting should also be conducted to ensure the narrative will be understood, will be accepted, and will resonate with the appropriate audiences and stakeholders prior to dissemination. The pretesting process may include red teaming/“wargaming,” expert panels, and focus groups or surveys (refer to Figure A-1).



Figure A-1. Potential Testing Pool

After pretesting and refinement, approval is granted once the commander feels the narrative captures the intent of the mission/operation/campaign. The narrative statement is included in the planning directive, ideally right after the mission statement.

g. Assess and Refine

(1) Once a narrative is associated with an event or series of events, regardless of the effects, it is very difficult and often inadvisable to change it. However, narratives can be refined and/or rebalanced to change the emphasis or create greater emotional appeal. Throughout the operation, the mission narrative will be continuously assessed to identify any requirement to refine it. This also ensures the mission narrative remains consistent with political guidance as the mission evolves. Assessment is also done to determine how operations/activities should be refined based on the effect they have on the narrative. Continuous assessment of operations and activities on the narrative is a critical function to mitigate unintended consequences.

UNITED STATES DRONE OPERATIONS IN PAKISTAN

For the United States, drone operations were an effective means to target officials, members, and affiliates of al Qaeda who posed an imminent threat of attack on the US homeland. They were also part of a longer standing narrative of the United States as a superior technological power, especially in war. The Pakistan media however, portrayed the drone strikes as killing thousands of civilians. Eventually, the drone strikes began to be seen by some as a war against Pakistanis and Muslims in general. In this example, although the drone strikes were executed in a bilateral manner with Pakistani officials, internal and rival political factors leveraged the same events to their advantage. This negative reaction, at the strategic level had to be carefully weighed against short-term tactical gains.

Various Sources

(2) Information forces, along with the JFC's J-2, support assessment efforts by analyzing open and classified sources of information to determine audience perspectives and reactions to joint force messages and physical activities. Engagements with the various audiences by the commander, staff, subordinates, and mission partners also provide useful feedback. Surveys, both those conducted by the joint force and those conducted by other stakeholders such as DOS, media, the HN, and mission partners, can provide quality feedback on how the narrative is resonating with audiences.

5. Changing the Narrative

a. Sometimes, it will be necessary to change the narrative. Some reasons to change a mission narrative include a change in policy, a change in conditions in the OE, or because the current mission narrative is detrimental to achieving objectives. When changing the narrative, it is important to remember that the joint force can control what it says about itself (the mission narrative), but it can only influence (not control) what audiences are

saying about the joint force. As a result, it may take time to overcome any negative effects that the previous narrative may have generated. Additionally, changing a narrative can cause audiences to question the resolve or credibility of the joint force so it should be done only after a careful consideration of the risk associated with not changing it.

b. Changing the narrative involves the same considerations and steps as developing the narrative above but also involves:

(1) Understanding how the current narrative is resonating with the relevant audiences. This includes understanding how operations are currently reinforcing unwanted perceptions.

(2) Clearly identifying and articulating the compelling reason to change. The rationale has to be communicated as part of the narrative.

(3) Identifying and communicating the desired or anticipated changes.

Intentionally Blank

APPENDIX B

INFORMATION STAFF ESTIMATE FORMAT

Originating Division, Issuing Headquarters

Place of Issue

Date-Time-Group, Month, Year

INFORMATION ESTIMATE NUMBER _____ *

References:

- (1) JP 3-04, *Information in Joint Operations*.
- (2) JP 5-0, *Joint Planning*.
- (3) Maps and charts.
- (4) Other pertinent documents.

1. Strategic Mission Narrative and Commander's Intent Two Levels Up

The strategic mission narrative conveys the commander's reasons and desired outcomes for the campaign/mission/operation along with its supporting themes. The strategic mission narrative explains the use of the military and puts global operations in context. The commander's intent identifies the major unifying efforts during the campaign or operation, the points, and events where operations must succeed to control or establish conditions in the JOA, and where other instruments of national power will play a central role. The intent must enable decentralized execution. It provides focus to the staff and helps subordinate and supporting commanders to take actions that achieve the commander's objectives without further orders, even when the operation does not unfold as planned.

2. Operational Mission Narrative and Unit Commander's Intent

The operational mission narrative nests under the strategic mission narrative. Operational mission narratives focus on the theater/region and seek to advance the legitimacy of the mission while countering adversary narratives. From the current planning guidance or orders, each unit commander develops a clear and concise expression of the purpose of the operation and the desired outcomes.

3. Desired State of the Joint Operations Area

Concisely express the desired state of the JOA within the expanded purpose statements as determined during operational design. Includes relevant aspects of the USG strategic

narrative to inform JFC objectives. Military Messaging Guidance is normally a component of the national strategic narrative. The estimate will include behavioral objectives and conditions linked to the desired state of the JOA. Objectives are written so that they inform the development of CCIRs.

4. Area of Interest

AOI is that area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. The AOI also includes areas where relevant actors reside that may not be adjacent to the JFC's JOA or AOI but from which they have the potential to affect the success of the JFC's mission. Include those relevant actors linked by common language, religion, and other cultural factors (e.g., diaspora enclaves, co-religionists) and/or that may have other objectives (e.g., political interest, business interest) that have the potential to affect the JFC's mission.

5. Mission

State the mission of the command as a whole, taken from the commander's mission analysis, planning guidance, or other statements.

6. Centers of Gravity

The information CFT expands the COG analysis approach to describe and prioritize relevant actors, including the joint force itself, during conditions of cooperation, competition, and armed conflict. Representatives from each of the joint functions contribute to COG analysis (e.g., the sustainment staff conduct analysis of transportation methods, routes, and numerous business interests for contracting within the JOA). The information planners consider sustainment input during COG analysis to gain a refined understanding of relevant actors, to include an assessment of their importance in achieving JFC's objectives, which then informs COA development, analysis, and selection. Based on COG analysis, planners recommend actions (to include communications) the joint force should take and what actions they should avoid taking in support of the JFC's objectives. Potentially, planners will nominate multiple COGs for simultaneous targeting based on the critical vulnerabilities of each. The joint force leverages information, to include the inherent informational aspects activities, to affect identified COGs. The joint force monitors COGs over time to gain a more nuanced understanding of how to attain enduring outcomes. The information CFT will help identify which USG and joint force activities require a sustained effort during COG analysis.

7. Situation and Considerations

a. Characteristics of the Environment. Summarize the analysis of the informational, physical, and human aspects of the environment by describing the different characteristics of objects, activities, or actors in the context of one another and of the broader environment. This summary helps identify the relevant actors the joint force needs to affect, how to use information to effectively impact those relevant actors, and what

friendly information the joint force needs to protect. As a minimum, use the following as references: the current intelligence estimate, CMO estimate, military police estimate, MISO estimate, and TAA. Depict the characterization in visual and narrative forms to communicate it to the commander, staff, and subordinate units.

(1) **Informational Aspects.** Describe how individuals, information systems, and groups communicate and exchange information. This description includes informational content that can be collected, transmitted, processed, stored, and displayed. Describe the formal and informal communication infrastructure and networks, kinship and descent relationships, licit and illicit commercial relationships, and social affiliations and contacts that collectively create, process, manipulate, transmit, and share information in an operational area and among relevant actors. These also include the inherent informational aspects of activities (i.e., the “body language” of activities), which are described in Chapter I, “Fundamentals of Information.” Describe the features and details, which include, but are not limited to, the size of a force and its types of capabilities; the communications about an activity (e.g., verbal and nonverbal communication, images, credible voice); and the duration, location, and timing of the activity.

(2) **Physical Aspects.** Describe the material characteristics of the JOA, natural and manufactured, that inhibit or enhance communication between people and between information systems. This includes physical features such as terrain and lines of communication that impact the transmission and processing of information. Physical aspects include territorial boundaries associated with governments’ obligations to provide security for their people. Physical aspects are critical elements of group identity and frame how tribes and communities form. Physical aspects also include the characteristics of the medium used in communication such as the material on which something is printed or the radio frequency and bandwidth used during broadcast. Other physical aspects are geographic features that can block or enable communication, provide protection, and obstruct or enable movement. Information infrastructure to include its capabilities, its organization, and how it impacts the content and flow of information, are also included in this description.

(3) **Human Aspects.** Describe how relevant actors (human and automated systems) interact with each other and with their environment. Human aspects frame how relevant actors perceive a situation from their world view. This frame is the basis of their perspective, from which they derive meaning to what they observe to understand the context of the world around them. Human aspects may include, but are not limited to, the language, social, cultural, psychological, and physical characteristics that shape a relevant actor’s behavior. Identify aspects that may be useful in anticipating how relevant actors in the JOA might behave under particular circumstances. Identify issues such as competition for territory and resources, contending wills, and injustice or lack of representation, which may be the root of the current problem or conflict. Identify the key linguistic, social, cultural, psychological, and physical elements that shape the behavior of relevant actors. This may include the character, tradition, and the objectives of relevant actors that suggest how they might behave under particular circumstances. Also included is identification of

the key influencers within the area and known linkages to organizations and groups that may support or challenge the commander's objectives.

(4) **Synthesis of Aspects.** An environment is characterized by its informational, physical, and human aspects. Explain how these three aspects influence and interact with each other. Include a description of likely methods of approach to gain access to communicate with the groups of interest. Through understanding relevant actor culture, economics, security, food, water, transportation, communication, relationships with other groups, and other relevant vulnerabilities and strengths, the joint force is more likely to gain and maintain communication with relevant actors. This approach leverages any means and combination of capabilities within the lawful parameters of the operation.

b. Enemy Forces

(1) **Strength and Disposition.** As a minimum, use the following as references to form a multisource description: the current intelligence estimate, CMO estimate, military police estimate, MISO estimate, and TAA.

(2) **Enemy Capabilities.** Describe enemy abilities to use information to reduce the effectiveness of friendly forces and inhibit the joint force from achieving its objectives. This includes enemy force's ability to disseminate propaganda and disinformation. Describe the known and suspected reach of enemy and adversary relationships known to influence action of those groups that can support or challenge the commander's objectives.

c. Friendly Forces

(1) **Present Disposition of Major Elements.** Include estimates of force strengths for those capabilities, operations, and activities that will be used to leverage information.

(2) **Own COAs.** State the proposed COAs under consideration; focus on the key tasks associated with the operations or plans. COAs are developed based on the operational mission narrative, restated mission, commander's intent, and planning guidance.

(3) **Probable Tactical Developments.** Review major deployments and logistics preparations necessary in all phases of the proposed operation.

(4) **Unit Status.** State known personnel, equipment, and training shortfalls, which may affect the ability to meet the developing situational requirements.

(5) **Assumptions.** State assumptions about the informational, physical, and human aspects of the situation made for this estimate. Do not repeat here the basic assumptions for the operation that have already been made and will appear in planning guidance and in the plan itself. State certain assumptions that may have been made concerning potential or likely vulnerabilities in preparing this estimate.

(6) **Special Features.** State here any special features not covered elsewhere in the estimate that may support or counter the commander's objectives.

(7) **Informational Capabilities, Operations, and Activities.** Describe capabilities, operations, and activities that use information and leverage information to affect behavior and impact the OE. This section includes authorities and permissions required to execute these information activities. All tasks of the information joint function should consider their contribution to joint maneuver. It is important to note that the following list of capabilities, operations, and activities employed to leverage information is not all-inclusive. From the multifunctional information perspective:

(a) **Key Leader and Other Engagements.** Describe scheduled and likely engagements (e.g., KLEs, civilian-to-civilian, military-to-military, civilian-to-military, military-to-civilian). Identify relationship and influence objectives. Specify capabilities and shortfalls for language, regional expertise, and culture knowledge and skills; and include COAs and approximate time necessary to mitigate capability gaps. Identify key leaders, develop messages, and describe options for ways and means (i.e., place, time, and event) of delivery, focused on interpersonal relationships. Understand the impact of the KLEs over time. Is the command getting what it perceives it needs to achieve objectives while attempting to build relationships and cooperative action?

(b) **PA.** Relevant overview from the PA estimate. Describe organic and partner PA capabilities relevant to inform tasks based on commander's objectives, including the location and capabilities of key PA units and teams. Describe PA communication and synchronization planning, execution, and assessment activities for the operation in alignment with the USG narrative. Describe the strategic and operational media environment and the critical factors that could impact the command's mission. Assess potential media presence, capabilities, and content, as well as national and international attitudes about the situation, command, and leaders. Analyze key audiences and their news and information expectations and how the command can best inform them. Provide an assessment of the public, social, and traditional media sentiment and the potential effects of joint operations on that sentiment. Consider the requirement to effectively communicate with the populace for whom the commander may become responsible. State known capabilities and shortfalls (to include access to relevant actors and audiences) and include COAs and approximate time necessary to mitigate capability gaps. Describe status of authorities relevant to PA activities.

(c) **CMO.** Relevant CMO overview from the estimates of the situation, to include area studies. Describe logistics and support infrastructure required to sustain CMO-contracted support by function and location, from interagency, HN, multinational, and NGO partners during shaping and follow-on phases of operations. Describe information approach to enhance whole-of-government effectiveness and work toward efficiency. Describe gaps remaining in the area study, assessment, and staff estimate. Identify the problems and estimate the risks to the commander's objectives. As required, provide updates to ongoing assessments, estimates, and area studies. As required, describe activities that may occur prior to, during, or subsequent to other military actions. Describe

the civil component of the JOA and identify underlying causes of instability within civil society. Identify gaps in functional specialty skills normally the responsibility of civil government. Describe CMO view of COG analysis. Describe status of authorities relevant to CMO activities.

(d) **Deception.** Describe competitor, adversary, and enemy relevant actors' impressions about friendly force dispositions, capabilities, vulnerabilities, and intentions to aid other staff members in understanding how to affect the opponent's drivers of behavior to mislead or induce them to behave in a manner advantageous to the joint force. This section should increase the understanding of other multifunctional planners who can suggest options to manipulate the opponent's intelligence collection, analysis, and dissemination systems. The information staff presents options for developing credible stories, identifies and orients on appropriate deception audience, and assesses the effectiveness of any deception effort. Thorough knowledge of the relevant actor and the relevant actor's decision-making processes informs options for all joint force activities. Planners describe focused approaches intended to cause the relevant actor to behave in a desired manner, not simply to be misled in their thinking and processing of their mission essential information. Describe status of authorities relevant to deception activities.

(e) **MISO.** Describe the characteristics of the operational area (from MISO perspective), the psychological impact of JFC's proposed COA, and key considerations for COA supportability. Describe MISO planning, execution, and assessment activities for the operation in support of JFC objectives. Identify hostile, friendly, and neutral target sets. Describe current status of organic and external influence capabilities. Identify critical shortfalls such as information/intelligence needs for the proposed MISO programs and ongoing TAA, availability of linguists, availability of indigenous personnel for employment with psychological operations personnel, or accessibility to reach selected TAs, and include COAs necessary to reduce their impact. Describe status of approval process and authorities to execute MISO.

(f) **OPSEC.** Assess the risk to preserving essential secrecy by identifying the crucial information and indicators that must be protected, assess the vulnerabilities to adversary collection and interpretation, and identify possible OPSEC countermeasures to mitigate vulnerabilities. Present options to highlight or conceal friendly intentions, capabilities, or activities to support joint force objectives. Include information that facilitates staff understanding of how to derive critical information. Recommend OPSEC planning guidance for inclusion in the commander's planning guidance. In conjunction with the intelligence joint function, during options development, integrate the estimated enemy's assessment of friendly operations, capabilities, and intentions with the rest of the information staff. Specifically, address any known opponent knowledge of the friendly operations covered in the basic plan. Identify indicators during plans and analysis of options. Describe indicators that opponents can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. Recommend OPSEC practices that balance the responsibility of accountability with the American public against the need to protect critical information and indicators.

(g) **JEMSO.** Describe the integration and synchronization of EW, EMS management, intelligence, and other mission areas to achieve EMS superiority, unity of effort, and the JFC's objectives. Describe future opportunities in time, space, and technology affecting a physical area to enable other activities that communicate or maneuver through the EMS, such as MISO, PA, or CO. Describe status of authorities relevant to JEMSO activities.

(h) **COMCAM.** Discuss status, capabilities, and locations of COMCAM forces providing mission support functions to the JFC. Describe gaps in capabilities tied to unsupported request for support within the JOA. Provide recommendations to fill specified requests for support.

(i) **Space Operations.** Describe space capabilities supporting the JFC. Describe the effects of hostile actions from both state and non-state actors on space support to the JFC. Describe activities to neutralize or reduce the effectiveness of hostile action against US, allied, and partner-nation space capabilities. Describe activities to reconstitute space capabilities. Recommend specific space operations tasks to support the JFC's objectives.

(j) **STO.** Acknowledge when STO may provide contribution to joint force operations.

(k) **CO.** Describe an integrated application of cyberspace forces and capabilities to support the management of information and the leveraging of information in and through cyberspace. Describe when threats in cyberspace will negatively impact the JFC's ability to assure system and network availability, information protection, and information delivery. Describe gaps in DODIN protection capabilities required to assure JFC essential functions and what is required to mitigate these gaps. Describe specific OCO that will support the JFC's objectives. Describe the authorities to be used or that will be required to execute the COA. Describe cyberspace-enabled activities that require special authorities or permissions for execution and describe the associated risk of conducting these activities.

(l) **Miscellaneous.** Include other capabilities, operations, and activities that leverage information, but are not considered elsewhere, that may influence selection of a specific COA. Include identity of known deficiencies of information force structure. Include identity of foreign and indigenous resources available or essential to support joint operations.

8. Information Analysis of Own Courses of Action

a. Analyze each COA considering the ways land, maritime, air, space, cyberspace, and special operations forces contribute to the three tasks of the information joint function; how the joint force can leverage the inherent informational aspects of activities to create relevant actor perceptions to achieve commander's objectives; and how the joint force will task organize and employ OIE units in support of objectives. This analysis should also identify how OIE will be used to amplify or conceal physical actions in a manner that increases or

decreases ambiguity and any friendly information systems or segments of friendly information networks that need to be prioritized for defensive actions based on the proposed COA. Finally, include a description of critical information and signatures that need to be protected for each COA along with recommended protection measures.

b. Examine each COA under consideration realistically from the standpoint of known and likely requirements versus available or programmed capabilities, climate and weather, hydrography, time and space, opponent capabilities, and other significant factors that may have an impact on the information situation as it affects each COA.

9. Comparison of Own Courses of Action

a. The information CFT considers each COA independently and evaluates/compares each against a set of criteria information planners helped develop and which contains information considerations. These criteria and their information considerations should be described here. The relative effectiveness and efficiency of each COA to address threats and avoid or mitigate hazards in or through the IE should also be described here. List the advantages and disadvantages of each proposed COA in leveraging information to achieve the JFC's objectives.

b. If necessary, use a worksheet similar to that used for the commander's estimate.

10. Conclusion

a. State which COA under consideration best leverages information in support of objectives.

b. Identify the major deficiencies in capabilities, operations, and activities that use information and leverage information to affect behavior and impact the OE which require the commander's attention. Include recommendations concerning the methods to eliminate or mitigate the negative effects of those deficiencies.

(Signed)

APPENDIX C

GUIDE FOR THE INTEGRATION OF INFORMATION IN JOINT OPERATIONS

Figure C-1 is a reference guide for the integration of information during the planning, execution, and assessment of joint operations.

Guide for the Integration of Information in Joint Operations

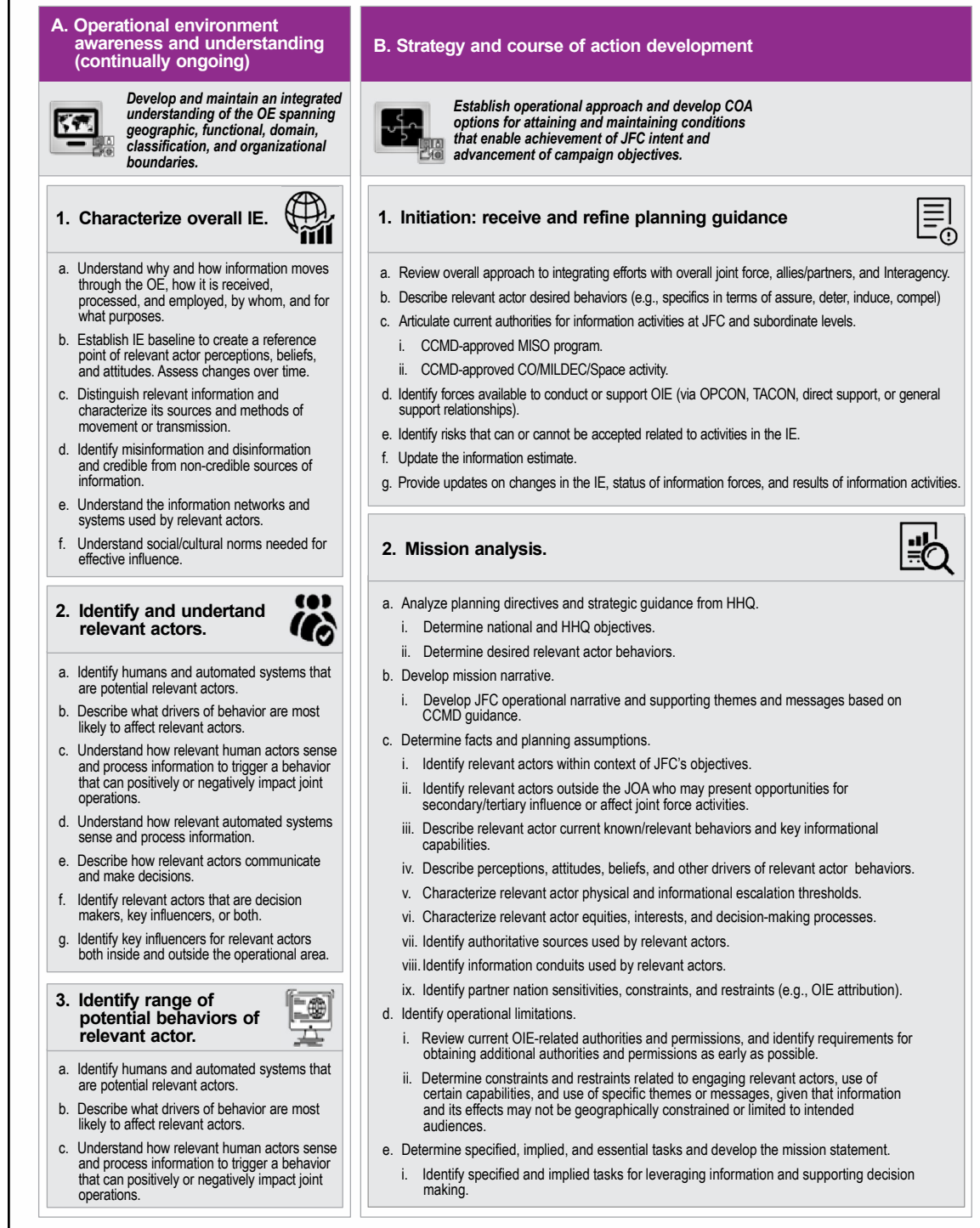


Figure C-1. Guide for the Integration of Information in Joint Operations

Guide for the Integration of Information in Joint Operations (cont.)

B. Strategy and course of action development (continued)



Establish operational approach and develop COA options for attaining and maintaining conditions that enable achievement of JFC intent and advancement of campaign objectives.

2. Mission analysis. (continued)



- f. Conduct initial force and resource analysis.
 - i. Identify the lead time to deploy information forces and specialized capabilities into theater or provide direct support to the joint force from outside the JOA.
 - ii. Request for forces or personnel with unique skills (e.g., linguists, sociocultural experts, social media experts, and automated-intelligence and machine-learning experts).
 - iii. Identify mission partners with information forces and specialized capabilities and/or capacities to fill joint force resource gaps.
 - iv. Evaluate requirements against existing or potential contracts or task orders.
- g. Develop military objectives.
 - i. Determine and articulate attainable behavioral goals.
 - ii. Develop MOEs and MOE indicators to assess how well the joint force leverages information.
 - iii. Identify indicators of trending success or failure into the monitoring and assessment plan.
- h. Develop COA evaluation criteria.
 - i. Information activities that produce desired behaviors in prioritized relevant actors.
 - ii. Information activities that protect the joint force from opponent attempts to undermine the joint force narrative or the legitimacy of the joint force mission and actions.
 - iii. Information activities that prevent, counter, and mitigate attempts to undermine joint force decision making and C2.
 - iv. Identify potential external information activities that negatively impact the achievement of the JFC's objectives.
- i. Develop risk assessment.
 - i. Identify strategic risks to JFC's narrative.
 - ii. Identify risk to joint force from malign influence.
 - iii. Refine analysis of risks to strategy, force, and mission. Develop mitigation approaches.
- j. Develop CCIRs.
 - i. Relevant actor behaving in a way that was not anticipated.
 - ii. Demonstration by an opponent of a new information capability against the joint force not foreseen during planning.
 - iii. Loss of access to communications channels used to inform or influence relevant actors.
 - iv. Emergent events that present a challenge to or opportunity for the JFC narrative.
 - v. Relevant actor desired behaviors and perceptions.
- k. Develop Information Estimate (see Appendix B).
- l. Prepare and deliver mission analysis brief.

3. COA Development



- a. Develop initial COA.
 - i. Establish approach to informing domestic, international, and internal audiences.
 - ii. Establish approach to influencing primary relevant actors.
 - iii. Establish approach to attacking and protecting information, information networks, and information systems.
 - iv. Validate operational objectives by developing preliminary MOE indicators for relevant actor behaviors and evaluating ability to assess them.
 - v. Identify forces desired to support informational power actions (including mission partners).
 - vi. Develop COA narrative, key themes, and messages.
- b. Refine COA (Based on COA analysis/wargaming).
 - i. Select relevant actors inside or outside JOA that may be opportunities for secondary or tertiary influence.
 - ii. Depict primary, secondary, and tertiary regions of influence inside and outside the JOA.
 - iii. Determine relative timing, tempo, intensity, scope, and linkage of physical force and informational power activities to create reinforcing effects in such a way to maximize their potential value.
 - iv. Identify opportunities to leverage/exploit PAI through MILDEC or other means.
 - v. Determine inherent informational aspects of activities and develop OIE approach for leveraging them to shape relevant actor behavior.
 - vi. Integrate OIE approaches into main and supporting lines of effort.
 - vii. Anticipate how joint force actions will resonate from physical domains to the IE, and how to respond to reactions by any potential relevant actors.
 - viii. Anticipate the opponent's OIE approaches and develop flexible options for countering them.
 - ix. Establish weights of effort for informational power and physical force.
- c. Establish timelines for executing proposed COA under available and accessible authorities.
- d. Identify OIE tasking mechanisms and associated timelines for employment to synchronize effects as required.
- e. Develop layered assessment plan.
 - i. Develop MOEs and MOE indicators for relevant actor behavior changes and overall strategic gain.
 - ii. Identify anticipated timeframes for gathering useful MOE indicators – initial reactions followed by long-term sentiment analysis.
 - iii. Develop collection requirements to observe MOE indicators.

4. COA analysis/wargaming



- a. Assess how relevant actors react to changes that each COA causes in the IE/OE.
- b. Anticipate how relevant actors might exploit PAI.
- c. Identify new relevant actors that may emerge as a result of the COA.
- d. Identify high priority relevant actors for influence.
- e. Evaluate ability to gather MOE indicators of relevant actor behavior changes within operationally relevant timeframes.

Figure C-1. Guide for the Integration of Information in Joint Operations (cont.)

Guide for the Integration of Information in Joint Operations (cont.)










C. Detailed Planning	D. Execution	E. Assessment
<p> <i>Develop detailed plans that affect relevant actor behavior through the integration of informational power with other capabilities and activities using assigned, attached, and supporting forces.</i></p> <p>1. Develop detailed plan. </p> <ol style="list-style-type: none"> Incorporate behaviorally-focused objectives into existing targeting processes and practices. Conduct ROE/JA review of proposed informational power effects. Draft collection plan to observe informational power-related MOE indicators. Develop integrated force package options to create desired effects. <ol style="list-style-type: none"> Identify and select specialized capabilities that can best enable/support other capabilities and activities (C2, fires, intelligence, movement and maneuver, sustainment, or protection). Identify and select specialized capabilities that can best leverage inherent informational aspects of activities. Identify and select specialized capabilities that can best directly affect relevant actor attitudes, perceptions, and other drivers of behaviors. Ensure access or ability to use specialized capabilities when required. Identify capability and capacity shortfalls related to the management and application of information and develop potential solutions. Develop synchronization matrix to align informational power and physical force (fires, movement and maneuver, sustainment, protection, intelligence, and intelligence) activities. 	<p> <i>Synchronize the creation of integrated effects. Adapt approach as evolving circumstances require.</i></p> <p>1. Check executive conditions. </p> <ol style="list-style-type: none"> Red-team informational power approaches prior to execution, leveraging up to date understanding of operational environment. <p>2. Monitor execution. </p> <ol style="list-style-type: none"> Collect MOE indicators and maintain understanding of the IE. Monitor how joint force activities are resonating through the IE. Update Information Estimate. <p>3. Manage and adapt execution. </p> <ol style="list-style-type: none"> Synchronize execution of OIE activities with other joint force activities. <ol style="list-style-type: none"> Maintain synchronization matrix. Align OIE activities within overall targeting cycle. Maintain updated narrative. Ensure operating within limits of applicable OIE authorities throughout execution. Identify and resolve conflicting OIE approaches with mission partners. Anticipate/adapt OIE approach to evolving situation in accordance with JFC objectives. Counter and compete with the opponent's emergent narratives and other OIE of concern. Integrate OIE into approach to handling escalation. 	<p> <i>Evaluate effects created against relevant actor perceptions, behavior, and capabilities. Identify new opportunities created to advance JFC objectives.</i></p> <p>1. Evaluate ability to execute OIE and synchronize with other activities (MOPs). </p> <ol style="list-style-type: none"> Determine if OIE and other activities were sequenced and executed as intended. Identify capability shortfalls and resource issues impeding effectiveness. Identify gaps in authorities/permissions impeding effectiveness. Identify communications (technical or human) issues that impeded effectiveness. <p>2. Evaluate MOE indicators and MOEs </p> <ol style="list-style-type: none"> Evaluate MOE indicators to characterize changes in relevant actor perceptions, attitudes, beliefs, and other drivers of behaviors. <ol style="list-style-type: none"> Ascertain if inherent informational aspects of activities were interpreted as intended. Track echoing/re-communication of JFC and DOD messaging (accurately or inaccurately). Evaluate OIE gain/loss. <ol style="list-style-type: none"> Establish extent to which non-overt actions were attributed to the joint force. Determine what was revealed about joint force capabilities through OIE activities, and if that met gain/loss expectations for those capabilities. Evaluate effects of component-level OIE in contributing to overall campaign-level joint force strategic gain.

Figure C-1. Guide for the Integration of Information in Joint Operations (cont.)

Guide for the Integration of Information in Joint Operations (cont.)

F. OIE toolbox: capabilities, operations, and activities for leveraging information



Legend

C2	command and control	MILDEC	military deception
CCIR	commander's critical information requirement	MISO	military information support operations
CCMD	combatant command	MOE	measure of effectiveness
Civ-mil	civil-military	MOP	measure of performance
CO	cyberspace operations	OE	operational environment
COA	course of action	OIE	operations in the information environment
DOD	Department of Defense	OPCON	operational control
EMSO	electromagnetic spectrum operations	ops	operations
HHQ	higher headquarters	OPSEC	operations security
IE	information environment	PAI	publicly available information
JA	judge advocate	ROE	rules of engagement
JFC	joint force commander	STO	special technical operations
JOA	joint operations area	TACON	tactical control
KLE	key leader engagement		

Figure C-1. Guide for the Integration of Information in Joint Operations (cont.)

Intentionally Blank

APPENDIX D REFERENCES

The development of JP 3-04 is based on the following primary references:

1. General

- a. Title 10, USC.
- b. Title 17, USC.
- c. Title 22, USC.
- d. Title 50, USC.
- e. Unified Command Plan.
- f. *(U) National Security Strategy of the United States of America, 2018.*

2. Department of Defense Publications

- a. SecDef Memorandum dated 15 September 2017, *Information as a Joint Function.*
- b. *(U) 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge.*
- c. *(U) National Military Strategy of the United States of America, 2018.*
- d. DODD 3600.01, *Information Operations (IO).*
- e. Department of Defense Instruction (DODI) O-3607.02, *Military Information Support Operations.*
- f. DODI 5040.02, *Visual Information (VI).*
- g. DODD 5111.01, *Under Secretary of Defense for Policy (USD[P]).*
- h. DODD 5111.10, *Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict.*
- i. DODD 5111.13, *Assistant Secretary of Defense for Homeland Defense and Global Security (ASD[HD&GS]).*
- j. DODD 5122.05, *Assistant to the Secretary of Defense for Public Affairs (ATSD[PA]).*

k. DODD 5135.02, *Under Secretary of Defense for Acquisition and Sustainment (USD[A&S])*.

l. DODD 5143.01, *Under Secretary of Defense for Intelligence and Security (USD[I&S])*.

m. DODM 5200.01, *DOD Information Security Program*.

n. DODM 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities*.

3. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 3050.01, *(U) Implementing Global Integration*.

b. CJCSI 3110.05F, *Military Information Support Operations Supplement to the Joint Strategic Capabilities Plan*.

c. CJCSI 3141.01F, *Management and Review of Campaign and Contingency Plans*.

d. CJCSI 3150.25G, *Joint Lessons Learned Program*.

e. CJCSI 3205.01D, *Joint Combat Camera (COMCAM)*.

f. CJCSI 3210.01C, *Joint Information Operations Proponent*.

g. CJCSI 3211.01F, *Joint Policy for Military Deception*.

h. CJCSM 3130.03A, *Planning and Execution Formats and Guidance*.

i. CJCSM 3500.04F, *Universal Joint Task Manual*.

j. JP 1, Volume 1, *Joint Warfighting*.

k. JP 2-0, *Joint Intelligence*.

l. JP 3-0, *Joint Campaigns and Operations*.

m. JP 3-08, *Interorganizational Cooperation*.

n. JP 3-12, *Joint Cyberspace Operations*.

o. JP 3-13.2, *Military Information Support Operations*.

p. JP 3-13.3, *Operations Security*.

- q. JP 3-13.4, *Military Deception*.
- r. JP 3-14, *Joint Space Operations*.
- s. JP 3-33, *Joint Force Headquarters*.
- t. JP 3-57, *Civil-Military Operations*.
- u. JP 3-60, *Joint Targeting*.
- v. JP 3-61, *Public Affairs*.
- w. JP 3-84, *Legal Support*.
- x. JP 3-85, *Joint Electromagnetic Spectrum Operations*.
- y. JP 4-02, *Joint Health Services*.
- z. JP 5-0, *Joint Planning*.
- aa. JP 6-0, *Joint Communications System*.

Intentionally Blank

APPENDIX E

ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication using the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

a. The lead agent for this publication is the Director for Global Operations (J-39). The Joint Staff doctrine sponsor for this publication is the Joint Staff Director of Operations (J-3).

b. The following staff, in conjunction with the joint doctrine development community, made a valuable contribution to the revision of this joint publication: lead agent, Joint Information Operations Warfare Center, Mr. Derek Elliot; Joint Staff doctrine sponsor, CDR Keith Adkins, Joint Staff, J-3; and LTC Joshua Darling, Joint Staff J-7, Joint Doctrine Branch.

3. Supersession and Cancellation

This supersedes and cancels JP 3-13, *Information Operations*, 27 November 2012 Incorporating Change 1, 20 November 2014. Relevant material from JP 3-13 has been incorporated into the main body and appendices of this publication. Accordingly, JP 3-13, *Information Operations*, will be removed from the joint doctrine hierarchy.

4. Change Recommendations

a. To provide recommendations for urgent and/or routine changes to this publication, please complete the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to js.pentagon.j7.mbx.jedd-support@mail.mil.

b. When a Joint Staff directorate submits a proposal to the CJCS that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Lessons Learned

The Joint Lessons Learned Program (JLLP) primary objective is to enhance joint force readiness and effectiveness by contributing to improvements in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy. The Joint Lessons Learned Information System (JLLIS) is the DOD system of record for lessons learned and facilitates the collections, tracking, management, sharing, collaborative resolution, and dissemination of lessons learned to improve the development and readiness of the joint force. The JLLP integrates with joint doctrine through the joint doctrine development process by providing lessons and lessons learned derived from operations, events, and exercises. As these inputs are incorporated into joint doctrine, they become institutionalized for future use, a major goal of the JLLP. Lessons and lessons learned are routinely sought and incorporated into draft JPs throughout formal staffing of the development process. The JLLIS Website can be found at <https://www.jllis.mil> (NIPRNET) or <http://www.jllis.smil.mil> (SIPRNET).

6. Releasability

LIMITED. This JP is approved for limited release. The authors of this publication have concluded that information in this publication should be disseminated on an as-needed basis and is limited to common access card holders. Requests for distribution to non-common access card holders should be directed to the Joint Staff J-7.

7. Printing and Distribution

Before distributing this JP, please e-mail the Joint Staff J-7, Joint Doctrine Branch, at js.pentagon.j7.mbx.jedd-support@mail.mil, or call 703-692-7273/DSN 692-7273, or contact the lead agent or Joint Staff doctrine sponsor.

a. The Joint Staff does not print hard copies of JPs for distribution. An electronic version of this JP is available on:

(1) NIPRNET Joint Electronic Library Plus (JEL+) at <https://jdeis.js.mil/jdeis/index.jsp> (limited to .mil and .gov users with a DOD common access card) and

(2) SIPRNET JEL+ at <https://jdeis.js.smil.mil/jdeis/index.jsp>.

b. Access to this unclassified publication is limited. This JP can be locally reproduced for use within the combatant commands, Services, National Guard Bureau, Joint Staff, and combat support agencies. However, reproduction authorization for this JP must be IAW lead agent/Joint Staff doctrine sponsor guidance.

APPENDIX F
(CLASSIFIED APPENDIX, PUBLISHED SEPARATELY)

Intentionally Blank

GLOSSARY

PART I—SHORTENED WORD FORMS (ABBREVIATIONS, ACRONYMS, AND INITIALISMS)

ACPD	Advisory Commission on Public Diplomacy (DOS)
AFCYBER	Air Force Cyber Command
AOR	area of responsibility
ARCYBER	United States Army Cyber Command
ASD(HD&GS)	Assistant Secretary of Defense for Homeland Defense and Global Security
ASD(SO/LIC)	Assistant Secretary of Defense for Special Operations /Low-Intensity Conflict
ATSD(PA)	Assistant to the Secretary of Defense for Public Affairs
BDA	battle damage assessment
C2	command and control
CA	civil affairs
CAG	civil affairs group (USMC)
CCDR	combatant commander
CCIR	commander's critical information requirement
CCMD	combatant command
CCP	combatant command campaign plan
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSOCOM	Commander, United States Special Operations Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CFT	cross-functional team
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CMF	Cyber Mission Force
CMO	civil-military operations
CMOC	civil-military operations center
CO	cyberspace operations
COA	course of action
COG	center of gravity
CO-IPE	cyberspace operations-integrated planning element
COM	chief of mission
COMCAM	combat camera
CONOPS	concept of operations
COS	chief of staff
CTF	counter threat finance
DC I	Deputy Commandant for Information (USMC)
DCO	defensive cyberspace operations

DISA	Defense Information Systems Agency
DJS	Director, Joint Staff
DMA	defense media activity
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODIN	Department of Defense information network
DODM	Department of Defense Manual
DOM	Directorate of Management
DOS	Department of State
EMS	electromagnetic spectrum
EMSO	electromagnetic spectrum operations
EW	electromagnetic warfare
EXORD	execute order
FFIR	friendly force information requirement
HN	host nation
IADS	integrated air defense system
IC	intelligence community
IE	information environment
IM	information management
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
J-1	manpower and personnel directorate of a joint staff
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
J-4	logistics directorate of a joint staff
J-5	plans directorate of a joint staff
J-6	communications system directorate of a joint staff
JAIC	Joint Artificial Intelligence Center
JEMSO	joint electromagnetic spectrum operations
JEMSOC	joint electromagnetic spectrum operations cell
JEWC	Joint Electromagnetic Warfare Center (USSTRATCOM)
JFC	joint force commander
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network (USCYBERCOM)
JIACG	joint interagency coordination group
JIATF	joint interagency task force
JIOC	joint intelligence operations center
JIOWC	Joint Information Operations Warfare Center
JIPOE	joint intelligence preparation of the operational environment

JISE	joint intelligence support element
JOA	joint operations area
JP	joint publication
JPEC	joint planning and execution community
JPG	joint planning group
JPP	joint planning process
JPSE	Joint Planning Support Element (USTRANSCOM)
JPSE-PA	Joint Planning Support Element-Public Affairs (USTRANSCOM)
JS	Joint Staff
JTF	joint task force
KLE	key leader engagement
KM	knowledge management
LOE	line of effort
LOO	line of operation
MAGTF	Marine air-ground task force (USMC)
MARFORCYBER	Marine Corps Forces Cyberspace Command
MCEN	Marine Corps Enterprise Network
MCIOC	Marine Corps Information Operations Center
MIG	Marine expeditionary force information group
MILDEC	military deception
MISO	military information support operations
MNF	multinational force
MOE	measure of effectiveness
MOP	measure of performance
NATO	North Atlantic Treaty Organization
NAVIFOR	Naval Information Forces
NGO	nongovernmental organization
NSC	National Security Council
OCO	offensive cyberspace operations
OE	operational environment
OIE	operations in the information environment
OPCON	operational control
OPE	operational preparation of the environment
OPLAN	operation plan
OPSEC	operations security
OSD	Office of the Secretary of Defense
PA	public affairs
PAG	public affairs guidance
PAO	public affairs officer

PIR	priority intelligence requirement
PMESII	political, military, economic, social, information, and infrastructure
POLAD	policy advisor
RFF	request for forces
RFI	request for information
16th AF	Sixteenth Air Force
SAP	special access program
SecDef	Secretary of Defense
SJA	staff judge advocate
SME	subject matter expert
SPOC	Space Operations Command (USSPACECOM)
STO	special technical operations
TA	target audience
TAA	target audience analysis
TIOG	theater information operations group (USA)
US	United States
USACAPOC	United States Army Civil Affairs and Psychological Operations Command
USASOC	United States Army Special Operations Command
USC	United States Code
USCYBERCOM	United States Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
US FCC	United States Fleet Cyber Command
USG	United States Government
USINDOPACOM	United States Indo-Pacific Command
USMC	United States Marine Corps
USSF	United States Space Force
USSPACECOM	United States Space Command
USTRANSCOM	United States Transportation Command
VI	visual information

PART II—TERMS AND DEFINITIONS

1. JP 3-04, *Information in Joint Operations*, 14 September 2022, Active Terms and Definitions

information environment. The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information. Also called **IE**. (Approved for incorporation into the DOD Dictionary.)

knowledge management. A discipline that integrates people and processes to create shared understanding, increased organizational performance, and improved decision making. Also called **KM**. (Approved for inclusion in the DOD Dictionary.)

operations in the information environment. Military actions involving the integrated employment of multiple information forces to affect drivers of behavior. Also called **OIE**. (Approved for inclusion in the DOD Dictionary.)

relevant actor. Individual, group, population, or automated system whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action. (Approved for inclusion in the DOD Dictionary.)

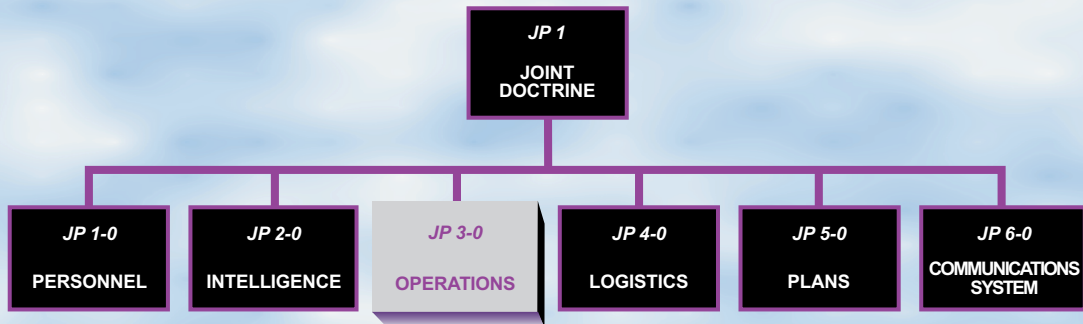
target audience. An individual or group selected for influence. Also called **TA**. (Approved for incorporation into the DOD Dictionary with JP 3-04 as the Source JP.)

2. Terms Removed from the DOD Dictionary

- **Supersession of JP 3-13, *Information Operations*, 27 November 2012; Incorporating Change 1, 20 November 2014:** information operations; information operations intelligence integration; information-related capability; information superiority

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-04** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

